



*Files are in Adobe format.  
Download the newest version from Adobe.*

## 2010 Biometrics Conference

*"The link between the Battlefield & Borders"*

**Arlington, VA**

**20 - 21 January 2010**

### [Agenda](#)

**Wednesday , January 20, 2010**

#### **WELCOME AND OPENING REMARKS**

- Mr. Jim Carlson, Chair, Industrial Committee on Biometrics; Executive Vice President, Iritech
- RADM Jeff Hathaway, USCG (Ret), Conference Chair; Vice President, L-1 Identity Solutions, Inc.

#### **KEYNOTE SPEAKER DoD Biometrics Task Force "Vision for the Future"**

- Dr. Myra Gray (slides, presentation notes), Director, Biometrics Task Force

#### **BIOMETRIC SCREENING PROGRAMS PANEL**

Moderator: RADM Jeff Hathaway, USCG (Ret), Conference Chair; Vice President, L-1 Identity Solutions, Inc.

Panelists:

- Mr. John Brennan, Senior Advisor, Bureau of Consular Affairs
- Mr. Steve Morris, Deputy Assistant Director, Criminal Justice Information Services Division, FBI
- Mr. Steve Yonkers, Deputy Assistant Director, Business Policy and Planning, US-VISIT Program

#### **PRIVACY ISSUES FIRESIDE CHAT**

Moderator: Ms. Beth Lavach, President, ELS and Associates

Panelists:

- Mr. Niels Quist, Advisor, Office of Privacy and Civil Liberties, U.S. Department of Justice
- Mr. Samuel Jenkins, Director, Defense Privacy Office, Office of the Secretary of Defense
- Mr. Steve Yonkers, Deputy Assistant Director, Business Policy and Planning, US-VISIT Program

**Thursday, January 21, 2010**

#### **TECHNOLOGIES & STANDARDS PANEL DISCUSSION**

Moderator: Mr. Glenn Hickok, Vice President, Federal, Cross Match Technologies, Inc.

Panelists:

- Dr. Patrick Flynn, Professor of Computer Science and Engineering; Concurrent Professor of Electrical Engineering, University of Notre Dame
- Dr. Sharla Rausch, Chief, Human Factors Division, Science & Technology Directorate, U.S. Department of Homeland Security
- Dr. John Butler, Biochemical Science Division, National Institute of Standards and Technology
- Dr. Jeff Salyards, MFS, Program Manager, Science & Technology, U.S. Army Criminal Investigation Laboratory

#### **FEATURED SPEAKER**

- Ms. Susan Ballou, Program Manager for Forensic Sciences, National Institute of Standards and Technology

#### **INTERNATIONAL PROGRAMS PANEL DISCUSSION**

Moderator: Mr. John Christensen, Account Executive, Northrop Grumman Corporation

Panelists:

- Mexico, Lic. Vicente Roqueñí, Minister Representative of the Secretariat of Governance, Embassy of Mexico to the United States
- Canada, Mr. Yves Levesque, MASINT & Biometrics, Chief of Defense Intelligence, Government of Canada
- Australia, Mr. Chris Dennis, Customs Officer, Australian Customs Service (ACS)

#### **PRIVATE SECTOR USE OF BIOMETRICS PANEL DISCUSSION**

Moderator: Mr. Jerry Jackson, Deputy General Manager, National Security & Defense Programs, National Interest Security Company

Panelists:

- Ms. Kathy Harman-Stokes, J.D., CIPP, Attorney Consultant on Biometric and Data Privacy Law, Stokes Law
- Mr. Nick Ivon, Director of Information Systems, Clark & Daughtrey Medical Group

# 2010 BIOMETRICS CONFERENCE

***“The link between the Battlefield & Borders”***

CONFERENCE  
HIGHLIGHTS  
INCLUDE:

Focused Panels/Fireside Chats:

- ▶ Biometrics Governance/Policy
- ▶ Biometric Screening Programs
- ▶ Privacy Issues
- ▶ Technology & Standards
- ▶ International Programs
- ▶ Private Sector use of Biometrics



JANUARY 20-21, 2010

[WWW.NDIA.ORG/MEETINGS/0860](http://WWW.NDIA.ORG/MEETINGS/0860)

SHERATON NATIONAL HOTEL ▶ ARLINGTON, VA

EVENT #0860

# WEDNESDAY, JANUARY 20

## BIOMETRICS GOVERNANCE/ POLICY FIRESIDE CHAT

This fireside chat will include updates on the continuing implementation of HSPD-24. Additionally, other emerging data/knowledge sharing initiatives will be covered.

## BIOMETRIC SCREENING PROGRAMS PANEL

This panel will be a discussion covering the continued growth of ongoing programs focused on “Finding the needle in the haystack”, connecting the terrorist watchlist and the “Thin blue line”; including successful matching protocols and continuing challenges.

**7:00 am - 6:15 pm** Registration Open

**7:00 am - 8:15 am** Continental Networking Breakfast

### 8:15 am **WELCOME AND OPENING REMARKS**

- ▶ MG Barry Bates, USA (Ret), *Vice President, Operations, NDIA*
- ▶ Mr. Jim Carlson, *Chair, Industrial Committee on Biometrics; Executive Vice President, Iritech*
- ▶ RADM Jeff Hathaway, USCG (Ret), *Conference Chair; Vice President, L-1 Identity Solutions, Inc.*

### 8:45 am **KEYNOTE SPEAKER**

**DoD Biometrics Task Force “Vision for the Future”**

- ▶ Dr. Myra Gray, *Director, Biometrics Task Force*

**9:15 am - 10:00 am** Networking Break

### 10:00 am **BIOMETRICS GOVERNANCE/POLICY FIRESIDE CHAT**

**Moderator:** Mr. Tom Giboney

**Panelists:**

- ▶ Mr. Monte Hawkins, *Director, Identity Management and Biometrics Policy, White House, National Security Staff*
- ▶ Mr. Al Miller, *Policy, Science and Engineering Advisor, Deputy Undersecretary of Defense for Policy Integration*
- ▶ Ms. Patricia Cogswell, *Executive Director, Screening Coordination Office, U.S. Department of Homeland Security*

### 11:25 am **INTRODUCTION TO FEATURED SPEAKER**

- ▶ Mr. Jim Carlson, *Chair, Industrial Committee on Biometrics; Executive Vice President, Iritech*

### 11:30 am **FEATURED SPEAKER**

- ▶ Gen Michael Hayden, USAF (Ret), *Former Director, CIA & Deputy Director, National Intelligence*

**12:00 pm - 1:00 pm** Networking Luncheon

### 1:00 pm **BIOMETRIC SCREENING PROGRAMS PANEL**

**Moderator:** RADM Jeff Hathaway, USCG (Ret), *Conference Chair; Vice President, L-1 Identity Solutions, Inc.*

**Panelists:**

- ▶ Mr. John Brennan, *Senior Advisor, Bureau of Consular Affairs*
- ▶ CDR Ty SchaeDEL, USN, *Deputy Chief, Enterprise Operations Division, Biometrics Task Force*
- ▶ Mr. Steve Morris, *Deputy Assistant Director, Criminal Justice Information Services Division, FBI*
- ▶ Mr. Steve Yonkers, *Deputy Assistant Director, Business Policy and Planning, US-VISIT Program*

# WEDNESDAY CONTINUED

**2:45 pm - 3:15 pm** Networking Break

## **3:15 pm **PRIVACY ISSUES FIRESIDE CHAT****

**Moderator:** Ms. Beth Lavach, *President, ELS and Associates*

### **Panelists:**

- ▶ Mr. Niels Quist, *Advisor, Office of Privacy and Civil Liberties, U.S. Department of Justice*
- ▶ Mr. Samuel Jenkins, *Director, Defense Privacy Office, Office of the Secretary of Defense*
- ▶ Mr. Steve Yonkers, *Deputy Assistant Director, Business Policy and Planning, US-VISIT Program*

**5:00 pm - 6:15 pm** Networking Reception

## **PRIVACY ISSUES FIRESIDE CHAT**

This structured forum will explore how current and emerging privacy policies related to identity management are being implemented, as well as discussion of future privacy issues that will challenge the growing use of biometric technology.

## **TECHNOLOGIES & STANDARDS PANEL**

This discussion will cover identification of current biometric technology gaps and new/future modalities; centralized vs. decentralized systems; fusion possibilities; and developing standards to accommodate tomorrow's technology.

# THURSDAY, JANUARY 21

**7:00 am - 4:00 pm** Registration Open

**7:00 am - 8:00 am** Continental Networking Breakfast

## **8:00 am **OPENING REMARKS****

## **8:10 am **INTRODUCTION TO KEYNOTE SPEAKER****

- ▶ Mr. Ramon Reyes, *Business Development Manager, MorphoTrak*

## **8:15 am **KEYNOTE SPEAKER****

- ▶ The Honorable James Clapper, *Under Secretary of Defense for Intelligence*

**8:55 am - 9:25 am** Networking Break

## **9:25 am **TECHNOLOGIES & STANDARDS PANEL DISCUSSION****

**Moderator:** Mr. Glenn Hickok, *Vice President, Federal, Cross Match Technologies, Inc.*

### **Panelists:**

- ▶ Dr. Patrick Flynn, *Professor of Computer Science and Engineering; Concurrent Professor of Electrical Engineering, University of Notre Dame*
- ▶ Dr. Sharla Rausch, *Chief, Human Factors Division, Science & Technology Directorate, U.S. Department of Homeland Security*
- ▶ Dr. John Butler, *Biochemical Science Division, National Institute of Standards and Technology*
- ▶ Dr. Jeff Salyards, MFS, *Program Manager, Science & Technology, U.S. Army Criminal Investigation Laboratory*

# THURSDAY CONTINUED

## INTERNATIONAL PROGRAMS PANEL DISCUSSION

This panel will discuss ongoing & future identity management programs of international colleagues, opportunities for collaboration and best practices.

## PRIVATE SECTOR USE OF BIOMETRICS PANEL DISCUSSION

This panel will provide examples of successful application of identity management systems used by industry today and systems planned and desired for future adaptation.

## CONFERENCE PLANNING COMMITTEE

- Chair: RADM Jeff Hathaway, USCG (Ret), *Vice President, L-1 Identity Solutions, Inc.*
- Mr. Steve Charles, *Program Manager, Raytheon Company*
- Mr. John Christensen, *Account Executive, Northrop Grumman Corporation*
- Mr. Magruder Dent, *Director, Federal Business Development, Aware, Inc.*
- Dr. Stephen Elliot, *Purdue University*
- Mr. Ron Fazio, *President, Integrated Forensic Laboratories, Inc.*
- Dr. Patrick Flynn, *Professor of Computer Science and Engineering; Concurrent Professor of Electrical Engineering, University of Notre Dame*
- Mr. Tom Giboney
- Mr. Jeff Hayes, *Director of Professional Services, Aware, Inc.*
- Mr. Glenn Hickok, *Vice President, Federal, Cross Match Technologies, Inc.*
- Mr. Jerry Jackson, *Deputy General Manager, National Security & Defense Programs, National Interest Security Company*
- Ms. Beth Lavach, *President, ELS and Associates*
- Ms. Rebecca Larson, *Lockheed Martin Corporation*
- Mr. Richard Ressler, *Principal, Booz Allen Hamilton*
- Mr. Ramon Reyes, *Business Development Manager, MorphoTrak*
- Mr. Steve Trost, *Director, DoD Programs, Daon*

### 11:15 am **INTRODUCTION OF FEATURED SPEAKER**

- Mr. Steve Trost, *Director, DoD Programs, Daon*

### 11:20 am **FEATURED SPEAKER**

- Ms. Susan Ballou, *Program Manager for Forensic Sciences, National Institute of Standards and Technology*

**11:45 am - 12:45 pm** Networking Luncheon

### 12:45 pm **INTERNATIONAL PROGRAMS PANEL DISCUSSION**

**Moderator:** Mr. John Christensen, *Account Executive, Northrop Grumman Corporation*

**Panelists:**

- Mexico, Lic. Vicente Roqueñí, *Minister Representative of the Secretariat of Governance, Embassy of Mexico to the United States*
- Canada, Mr. Yves Levesque, *MASINT & Biometrics, Chief of Defense Intelligence, Government of Canada*
- Australia, Mr. Chris Dennis, *Customs Officer, Australian Customs Service (ACS)*
- Netherlands, Mr. Mark Frijlink, *Project Leader, Innovation of Border Management, Immigration and Naturalization Service (Invited)*

**2:00 pm - 2:30 pm** Networking Break

### 2:30 pm **PRIVATE SECTOR USE OF BIOMETRICS PANEL DISCUSSION**

**Moderator:** Mr. Jerry Jackson, *Deputy General Manager, National Security & Defense Programs, National Interest Security Company*

**Panelists:**

- Ms. Kathy Harman-Stokes, J.D., CIPP, *Attorney Consultant on Biometric and Data Privacy Law, Stokes Law*
- Mr. Nick Ivon, *Director of Information Systems, Clark & Daughrey Medical Group*
- Mr. Andy Kemp, *Homeland Defense / National Programs, Apple, Inc.*

### 3:45 pm **CLOSING REMARKS**

- RADM Jeff Hathaway, USCG (Ret), *Conference Chair; Vice President, L-1 Identity Solutions, Inc.*



With the trust and confidence in individual identities provided by L-1 Identity Solutions, our customers can better guard the public against global terrorism, crime and identity theft fostered by fraudulent identity.

Leveraging the industry's most advanced multi-modal biometric platform for finger, face, palm and iris recognition, our solutions provide a circle of trust around all aspects of an identity and the credentials assigned to it. This includes proofing, enrollment, issuance and usage.

L-1 also provides convenient and secure fingerprinting service centers across the U.S. and Canada for processing civilian enrollment and credentialing for government-licensed jobs. The government consulting division completes the L-1 services portfolio, offering a diverse set of services that encompass the most important areas of security and intelligence in the U.S. today.

Learn more about our solutions for federal initiatives, programs and agencies:

- Homeland Security Presidential Directive 12 (HSPD-12) Compliance: NIST and GSA certified components and turnkey solutions and services for enrollment and card issuance
- Department of Defense/Intelligence: Finger, face and iris capabilities for use in theater and on base, and for personnel credentialing and identity management
- Passport and Visa Solutions: End to end capabilities for enrollment, fraud prevention, card and document production
- Solutions for Other Credentialing Programs – HAZMAT, TWIC, RT: Turnkey components and services for enrollment and card issuance

For more information, visit [www.l1id.com](http://www.l1id.com) or email [info@l1id.com](mailto:info@l1id.com).



MorphoTrak is a trusted partner for biometric and identity management technologies provided to the U.S. and Canadian governments. Working closely with agencies such as the FBI, DHS, DOD, RCMP and CATSA, MorphoTrak protects citizens at home and abroad by providing proven identity solutions that are backed by over 30 years of innovation in biometric and identity management technologies. With 130 biometric systems installed in 72 countries and 125 million secure credentials delivered, MorphoTrak has the knowledge and experience needed to assist integrators and agencies in creating a layered approach to homeland security. Further proof of MorphoTrak's excellence is the NIST testing that consistently places MorphoTrak's algorithms as top performers in fingerprint identification, as well as facial and iris recognition and the fusion of the two.

Formed from the merger of Sagem Morpho Inc. and Motorola's biometric division, Printrak, MorphoTrak has products and solutions that address the law enforcement, border control, civil identification, facility/IT security and access control markets. MorphoTrak and its global parent -- Sagem Sécurité -- are leading innovators in large fingerprint identification systems, facial and iris recognition, as well as identification technologies such as smartcards, secure travel documents, e-passports, and drivers' licenses. MorphoTrak employs over 450 persons, with headquarters near Washington D.C., engineering facilities in Anaheim, CA and Tacoma, WA, and field offices in Albany, NY and Austin, TX. Please visit <http://www.morphotrak.com> or call 1-800-601-6790 for more information.

## DISPLAYING COMPANIES INCLUDE:

AOptix Technologies, Inc.  
Aware, Inc.  
Cogent Systems  
Cross Match Technologies  
Daon, Inc.  
Defense Technical Information Center  
Hitachi America, Ltd.  
Iritech, Inc.  
Isilon Systems  
L-1 Identity Solutions, Inc.  
Maxvision  
MorphoTrak  
NetApp  
Novell, Inc.  
Sarnoff Corporation  
Science Applications International Corporation  
Smartmatic  
University of Windsor, IDIR  
ViaSim Solutions  
WCC Smart Search and Match

## THANK YOU TO OUR SPEAKERS!

In appreciation of our speakers at the 2010 Biometrics Conference,  
NDIA will make a donation to the Wounded Warrior Project,  
[www.woundedwarriorproject.org](http://www.woundedwarriorproject.org)



# THANK YOU TO OUR SPONSORS!



2010

# BIOMETRICS CONFERENCE

The Link Between The  
Battlefields & Borders

Susan Ballou: Program  
Manager  
NIST/OLE

1995 –



# DNA FUNDING - THE REPORT....

February 18, 2009

# NAS REPORT RECOMMENDATIONS

- ◉ #1: Establishing the National Institute of Forensic Science (NIFS)
  - Congress should establish and appropriate funds for an independent federal entity to oversee all forensic science activities.
- ◉ #2: Establish standard terminology to be used in reporting on and testifying about the results of forensic science investigations. Utilize model laboratory reports.

# NAS REPORT RECOMMENDATIONS

- ◉ #3: Fund peer reviewed research
  - Demonstrate the validity of methods
  - Establish the limits of reliability and accuracy that methods can expect to achieve
  - Quantifiable measures of uncertainty in conclusions
  - Automated techniques
- ◉ #4: Remove all public forensic laboratories and facilities from the administrative control of law enforcement agencies or prosecutor's offices.

# NAS REPORT RECOMMENDATIONS

- #5: Research on human observer bias and sources of human error
- #6: Develop tools for advancing measurement, validation, reliability, information sharing, and proficiency testing
  - Standards should reflect best practices and serve as accreditation tools.
- #7: Mandatory:
  - Laboratory accreditation
  - Certification of all forensic science professionals

# NAS REPORT RECOMMENDATIONS

- ◉ #8: Establish QA/QC procedures for all forensic laboratories.
- ◉ #9: Establish a national code of ethics and mechanisms for enforcement.
- ◉ #10: Improve and develop graduate education programs to include law schools
- ◉ #11: Improve medicolegal death investigation

# NAS REPORT RECOMMENDATIONS

- #12: Achieve nationwide fingerprint data interoperability.
  - Standards for representing and communicating image and minutiae data
  - Baseline standards to be used with computer algorithms
  
- #13: Establish a network to manage and analyze evidence from events that affect homeland security.

# President Vice President

Office of Science and Technology Policy

**OSTP**

National Science and Technology Council

**NSTC**

**Committee on Science**

**Sub Committee on Forensic Science**

**Interagency Working Groups  
(IWGs)**

# 5 IWGS

1. Certification, Accreditation and Licensing
2. Education and Ethics
3. Research, Development, Evaluation and Testing
4. Standards, Practices, and Protocols
5. Outreach

## **ACTIONS:**

- **What should be standardized?**
  - Specific techniques?
  - Reporting criteria?
  - Language used in reports?
  - Discovery information?
  - Evidence management?

## ***ACTIONS:***

- **Inventory Existing**
  - **Standards**
  - **Research**
  - **Training**
  - **Education**
  - **Accreditation**
  - **Certification**
- **Conduct a gap analysis**

# THROUGH LEADERSHIP SET HIGH ETHICAL STANDARDS

Thank you  
Susan Ballou  
[susan.ballou@nist.gov](mailto:susan.ballou@nist.gov)  
301-975-8750



# BIOMETRIC SCREENING PROGRAMS



# Bureau of Consular Affairs Biometric Programs

## Current Programs

- BioVisa Program – 10 Fingerprint Enrollment of Visa Applicants
- Facial Recognition Checks for Visas

# Bureau of Consular Affairs Biometric Programs

Programs Under Development

- Facial Recognition for Passports

Concepts Being Piloted

- Iris Recognition for Visas

# BioVisa & US-VISIT

- In 2003, in collaboration with US-VISIT, DOS began the BioVisa Program.
- The program started with the collection of two fingerprints that were checked against the DHS IDENT system.
- By 2007 this program had transitioned completely to a ten print collection with checks against both IDENT and the FBI's IAFIS system.

# Facial Recognition and Visas

- Facial Recognition checks have been used in visa processing since 2003.
- Our program began with checks against limited classes of visa applicants and has grown into the largest facial recognition system in the world.

# Facial Recognition and Visas

- In addition to watchlist checks, new visa photos are run against our visa records to search for potential identity fraud.
  - We have large holdings of visa record photos that predate fingerprint collection.
  - There are 78 million photos in our enrolled database.
- In FY 2009 we expanded our FR program to include all new visa application photos.

# Next Steps in Facial Recognition

- We did over 5 million FR checks of visa applications in FY 2009 and we are poised to significantly expand this number.
- We are launching a program of facial recognition checks for passport applications, now in a pilot phase.

# Facial Recognition and Passports

- The systems and infrastructure we have developed to do facial recognition checks of visas can be adapted to perform checks of passport photos.
- As with visa photographs, the FR checks can perform two main tasks:
  - Checks against watchlists that have associated photographs
  - Checks against the enrolled database to detect identity fraud.

# Facial Recognition and Passports

- In the past five years passport application numbers have doubled over the volume seen a decade ago.
- In FY 2009, 13.48 million passports were issued. In FY 2008, 16.2 million and in FY 2007, 18.38 million.
- Adding facial recognition checks into our passport procedures will significantly increase the size of our FR program.

# Facial Recognition and Passports

- Our pilot operations will allow us to assess the impact of FR procedures on passport processing and on the systems and human resources we use for FR.
- Our goal is a program to check all new applications against a sufficient range of records to produce significant benefits in fraud detection and watchlist coverage.

# Iris Recognition and Visas

- We have begun a pilot visa processing operation that uses iris recognition.
- This pilot is being run in cooperation with the Department of Defense, which holds iris enrollment records that can facilitate visa processing.
- The pilot will allow us to assess the technological and operational impacts of using iris recognition in visa processing.



# DNA Biometrics:

## *Standards and Technology*

**John M. Butler and Peter M. Vallone**

National Institute of Standards and Technology



NDIA Biometrics Conference (Arlington, VA)  
January 21, 2010

# Acknowledgments

- **NIST DNA Biometrics Team:**



Pete Vallone



Erica Butts



Kristen Lewis

- **FBI funding** through an interagency agreement with the NIST Information Access Division
- Early efforts with rapid PCR funded by Interagency Agreement 2008-DN-R-121 between the **National Institute of Justice** and NIST Office of Law Enforcement Standards

**NIST Disclaimer:** Points of view are ours and do not necessarily represent the official position or policies of the US Department of Justice or the National Institute of Standards and Technology. Certain commercial equipment, instruments and materials are identified in order to specify experimental procedures as completely as possible. In no case does such identification imply a recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that any of the materials, instruments or equipment identified are necessarily the best available for the purpose.

# Outline

- Importance of standards
  - in support of technology growth/application
- DNA as a biometric modality
  - advantages & challenges
- DNA basics
- NIST efforts with DNA
- Summary & future prospects with DNA

# National Security Presidential Directive and Homeland Security Presidential Directive (NSPD-59 / HSPD-24)

## Biometrics for Identification and Screening to Enhance National Security

- This directive establishes a framework to ensure that Federal executive departments and agencies (agencies) **use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals** in a lawful and appropriate manner, while respecting their information privacy and other legal rights under United States law.

**Signed by President Bush – June 5, 2008**

<http://www.biometrics.gov/Documents/NSPD59%20HSPD24.pdf>

# Importance of Standards

- **Interoperability** (data sharing) is facilitated
  - Example: common core DNA markers used in forensics
- **Quality** is enhanced
  - Example: FBI Quality Assurance Standards for forensic DNA testing laboratories
- **Technology** is enabled
  - Example: commercial vendors have target goals for product development

# Characteristics of a Biometric

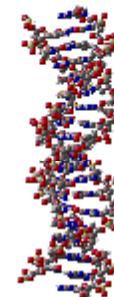
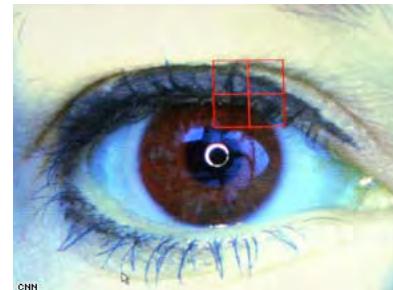
- Universality
  - each person should have the characteristic
- Uniqueness
  - how well the biometric separates individuals from another
- Permanence
  - how well a biometric resists aging and variance over time
- Collectability
  - ease of acquisition for measurement

# Current Biometrics

Some commonly measured features

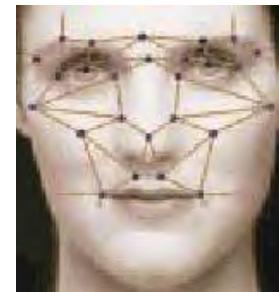
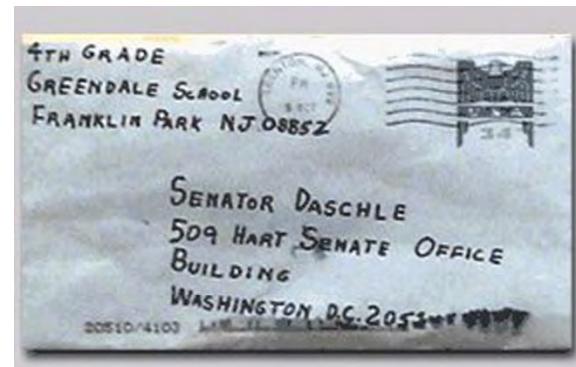
- Physical

- Fingerprints (Palm/hand geometry)
- Face
- Iris, retinal
- Odor/scent
- **DNA**



- Behavioral

- Gait
- Voice
- Vein (IR thermogram)
- Hand geometry
- Handwriting



# We are finding new ways to use DNA...

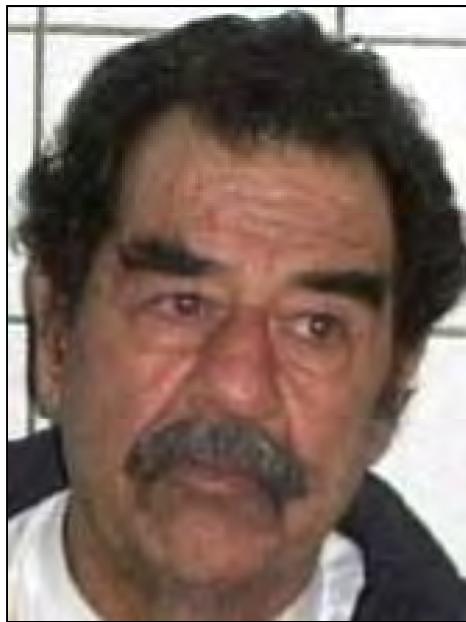
BIZARRO

We're taking back your first place ribbon. —We found traces of your parents' DNA all over your science fair project.



# DNA can be Viewed as the Ultimate Biometric

Captured December 13, 2003



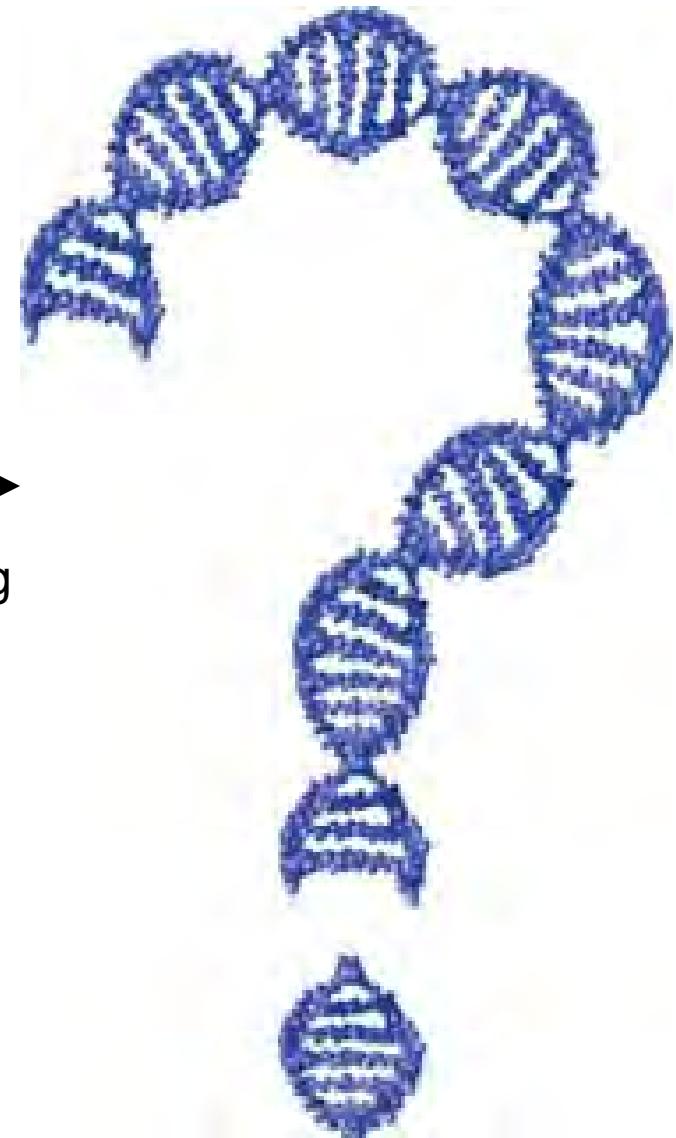
**Is this man really  
Sadaam Hussein?**

**Matching Y-STR  
Haplotype Used to  
Confirm Identity**



(along with allele sharing  
from autosomal STRs)

**Relatives Used  
to Confirm  
Identity**



# DNA Typing as a Biometric

## *Advantages*

- High level of accuracy (Gold Standard)
- Solid foundation of forensic DNA testing (population stats, genetics, molecular biology, court acceptance)
- **Kinship determination**
- Potential use for:
  - Phenotype (traits)
  - Ancestry

## *Challenges*

- Expensive
- **Time consuming**
- Sample collection (invasive, stability)
- Technical expertise required for analysis
- Low level template, mixtures, PCR inhibition

# The Desire is There...

The screenshot shows a news article from the July 2009 issue of National Defense magazine. The article is titled "Wanted: One Affordable Field-Ready DNA Testing Device" and is written by Stew Magnuson. The article discusses the potential use of affordable DNA testing devices in refugee camps and overseas adoption scenarios.

**National Defense** > Archive > 2009 > **July**

**Security Beat**

**Wanted: One Affordable Field-Ready DNA Testing Device**

**July 2009**

By Stew Magnuson

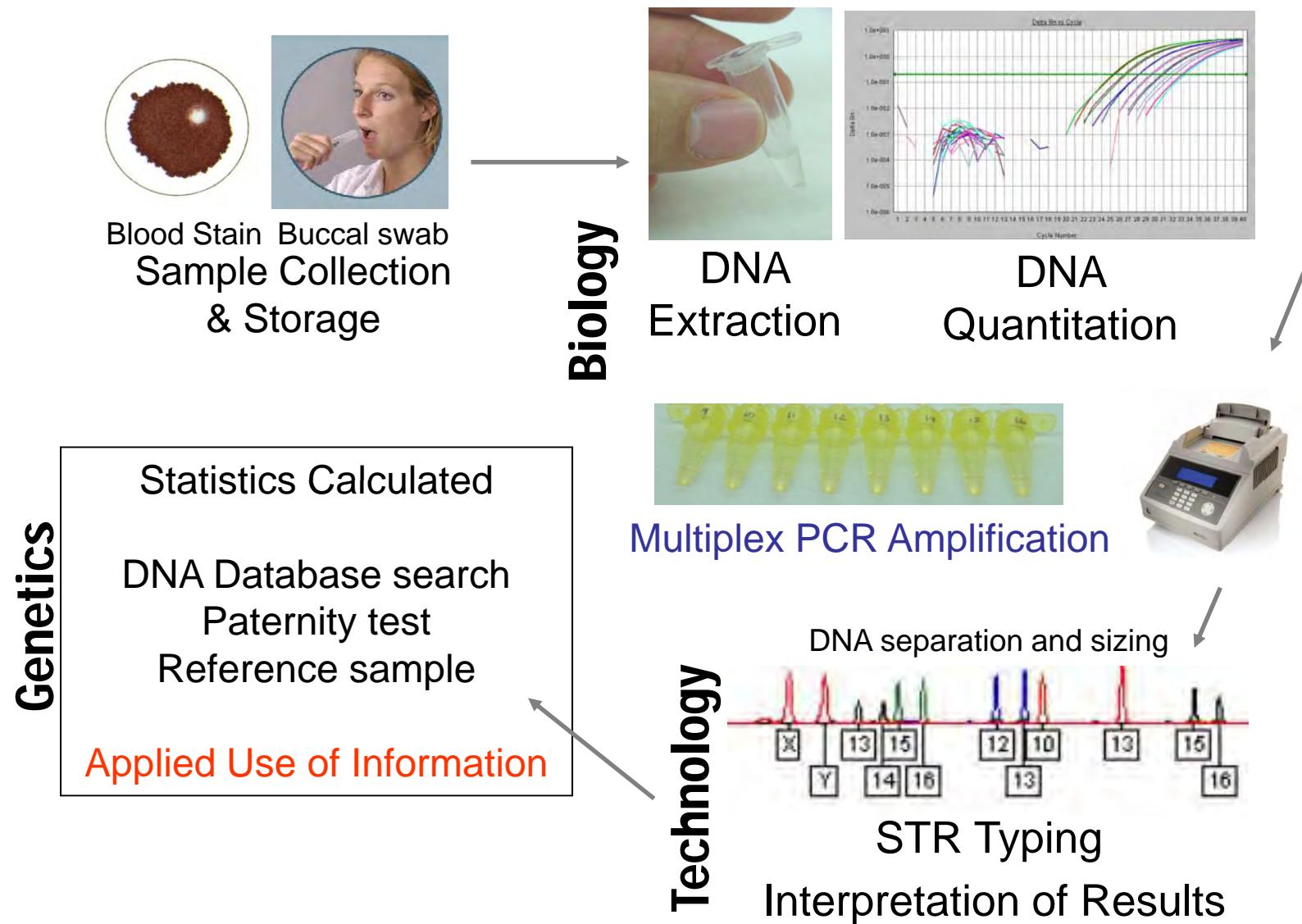
<http://www.nationaldefensemagazine.org/archive/2009/July/Pages/WantedOneAffordableField-ReadyDNATestingDevice.aspx>

- Use in refugee camps to confirm family relationships for asylum seekers (~80% fraud)
- Prevention of overseas adoption fraud where women may kidnap another's child in a baby-selling scheme

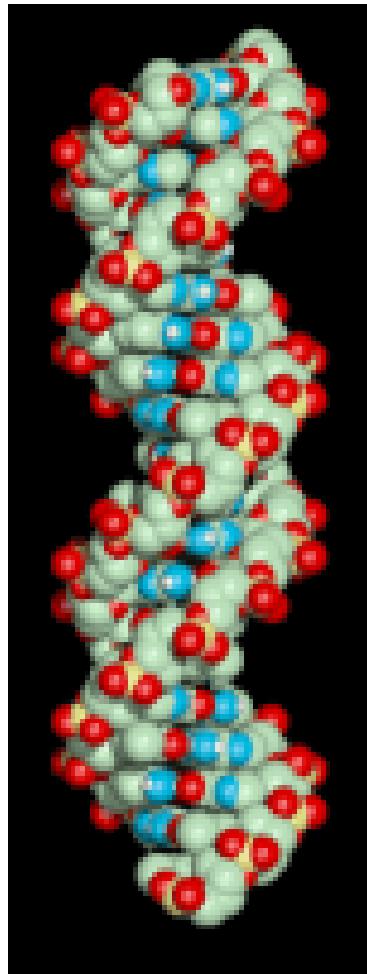
**Want result for <\$100 per test in <45 minutes**

# Steps in Forensic DNA Analysis

*Usually 1-2 day process (a minimum of ~8 hours)*

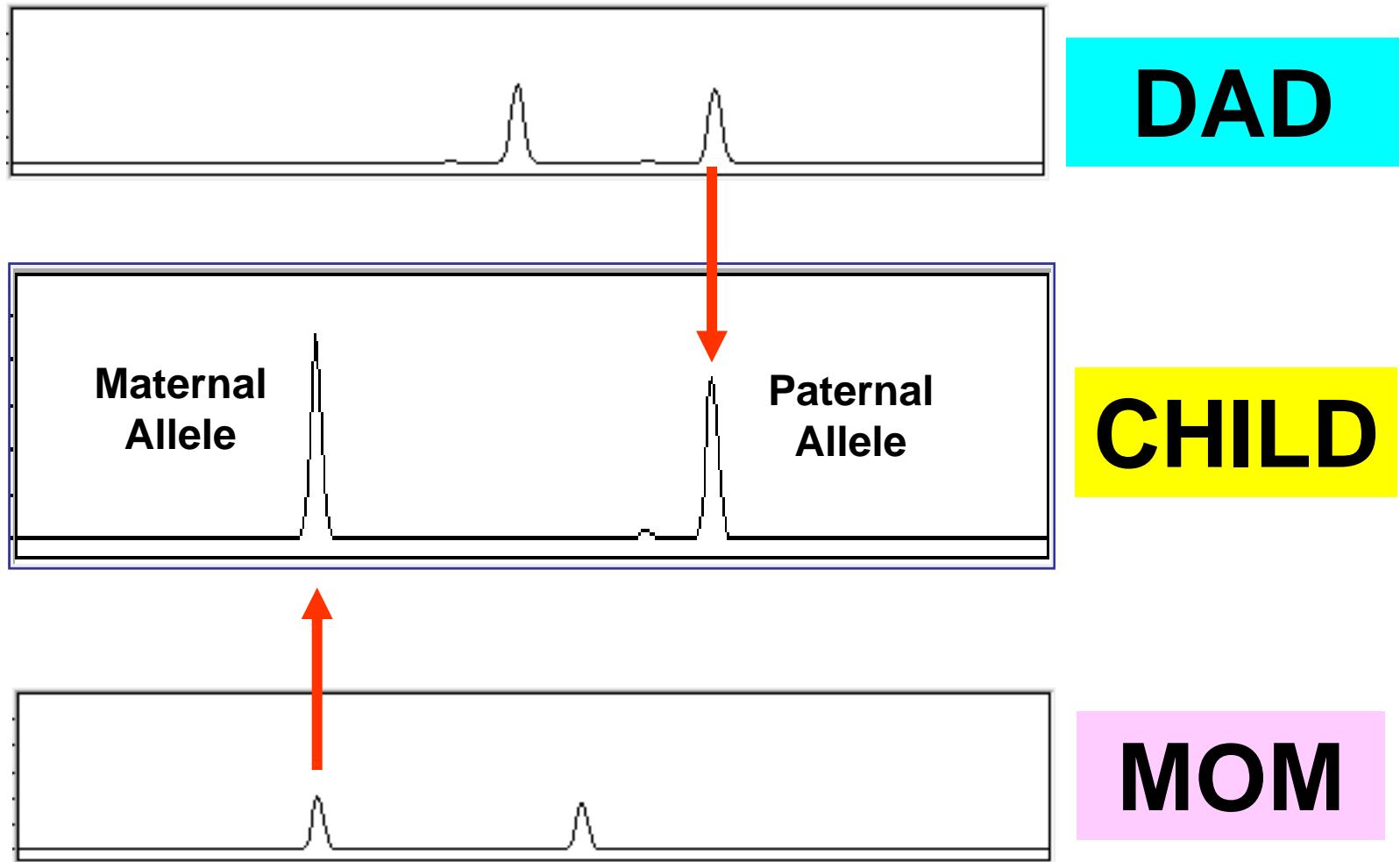


# Characteristics of DNA



- Each person has a unique DNA profile (except identical twins).
- Each person's DNA is the same in every cell.
- An individual's DNA profile remains the same throughout life.
- Half of your DNA comes from your mother and half from your father.

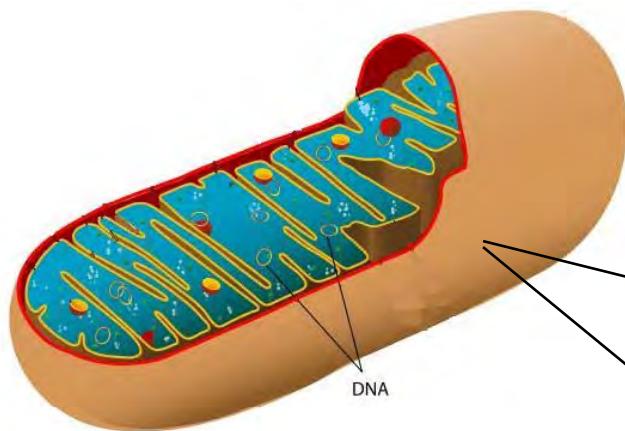
# Inheritance Pattern of DNA Profiles



**Result from a Single Locus (specific region of DNA)**

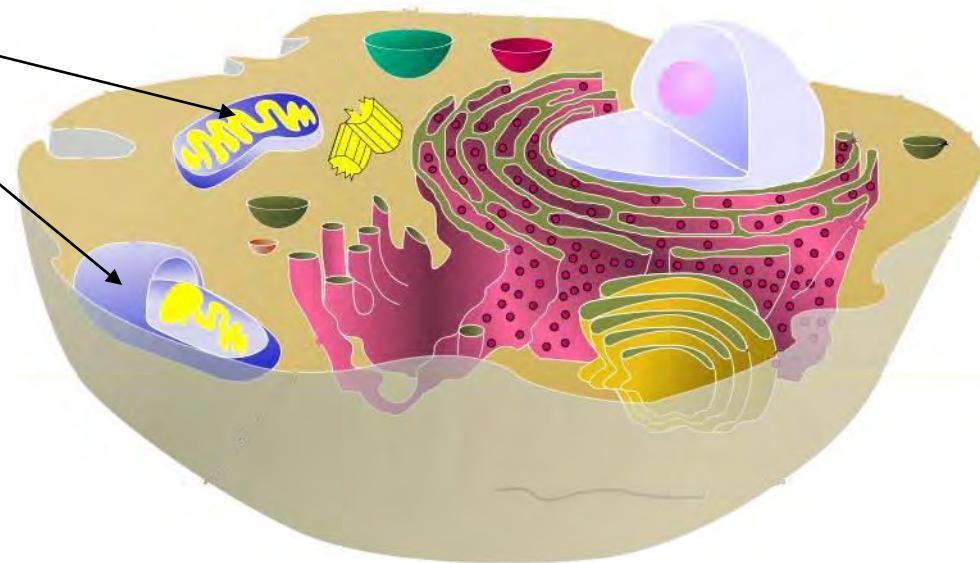
# The Human DNA Genome within a Cell

[http://en.wikipedia.org/wiki/Image:Diagram\\_of\\_an\\_animal\\_mitochondrion.svg](http://en.wikipedia.org/wiki/Image:Diagram_of_an_animal_mitochondrion.svg)



**Mitochondria = the power houses for the cell (hundreds per cell)**

**The Nucleus = control center for the cell (one per cell)**



[http://en.wikipedia.org/wiki/Image:Biological\\_cell.svg](http://en.wikipedia.org/wiki/Image:Biological_cell.svg)

**Mitochondrial DNA**  
(16,569 bp)

**Inherited from only  
your mother**

**Nuclear DNA**  
(3.2 billion bp)

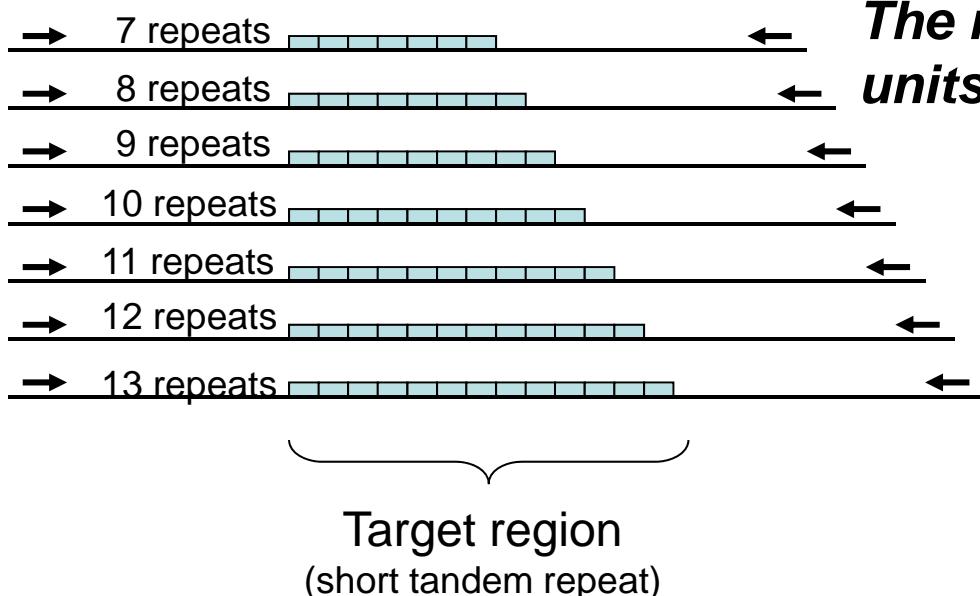
**Inherited from both  
your mother and your father**

# Short Tandem Repeat (STR) Markers

*An accordion-like DNA sequence that occurs between genes*

TCCCAAGCTCTTCCCTCTTCCCTAGATCAATACAGACAGAAGACA  
GGTGG**GATA**TAGATAGATAGATAGATAGATAGATAGATAGATA  
**GATA**TCATTGAAAGACAAAACAGAGATGGATGATAGATACATGC  
TACAGATGCACAC

= 11 GATA repeats (“11” is all that is reported)

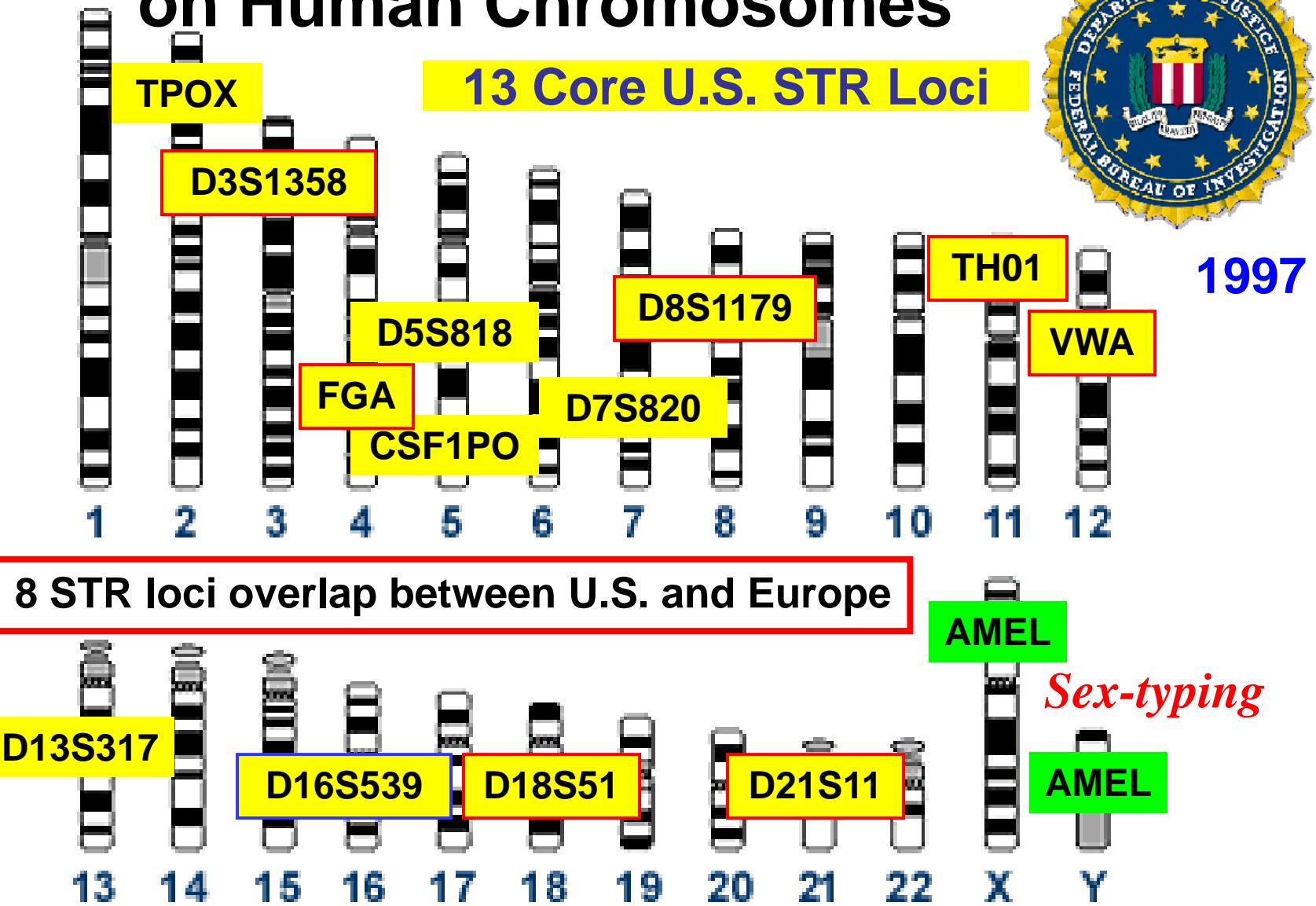


*The number of consecutive repeat units can vary between people*

The FBI has selected **13 core STR loci** that must be run in all DNA tests in order to provide a common currency with DNA profiles

## Core STR Loci for the United States

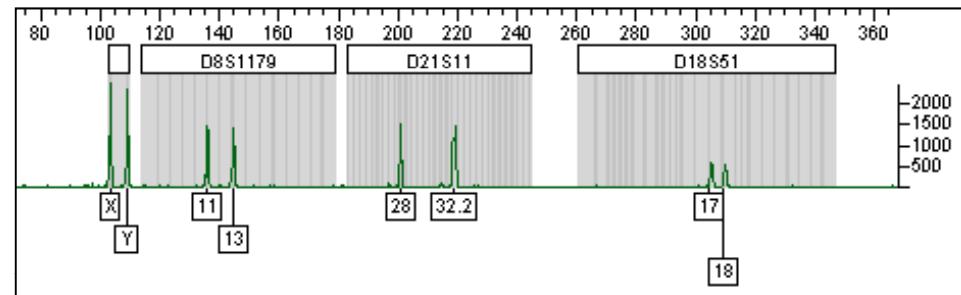
# Position of Forensic STR Markers on Human Chromosomes



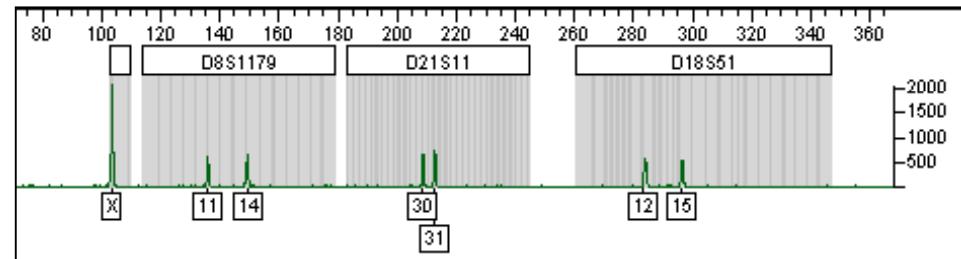
# STR Results

- Individuals will differ from one another in terms of their STR profile
- STR genotype can then be put into an alpha numeric form for search on a DNA database

**Individual #1**



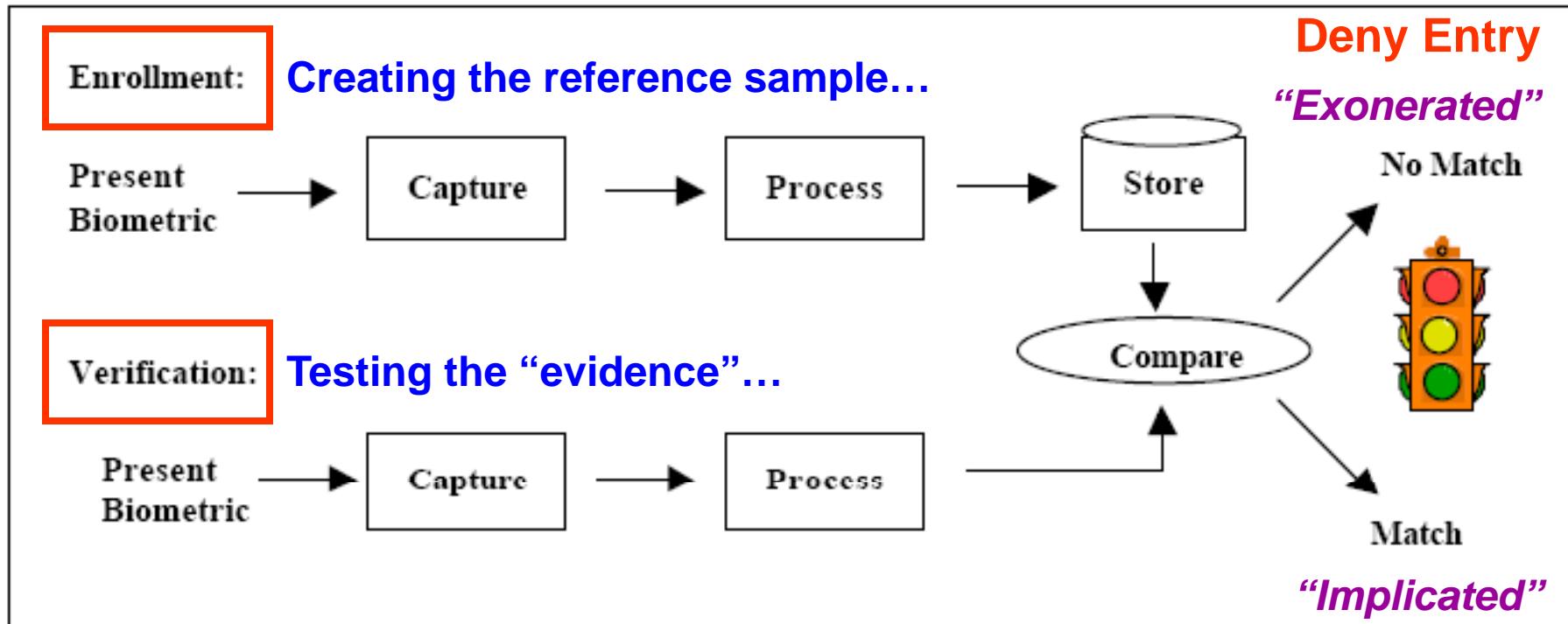
**Individual #2**



**What would be entered into a DNA database for searching:**

	<u>AMEL</u>	<u>D8S1179</u>	<u>D21S11</u>	<u>D18S51</u>
Individual #1	X, Y	11, 13	28, 32.2	17, 18
Individual #2	X, X	11, 14	30, 31	12, 15

# DNA within the Biometric Model



<http://www.itl.nist.gov/div893/biometrics/Biometricsfromthemovies.pdf>

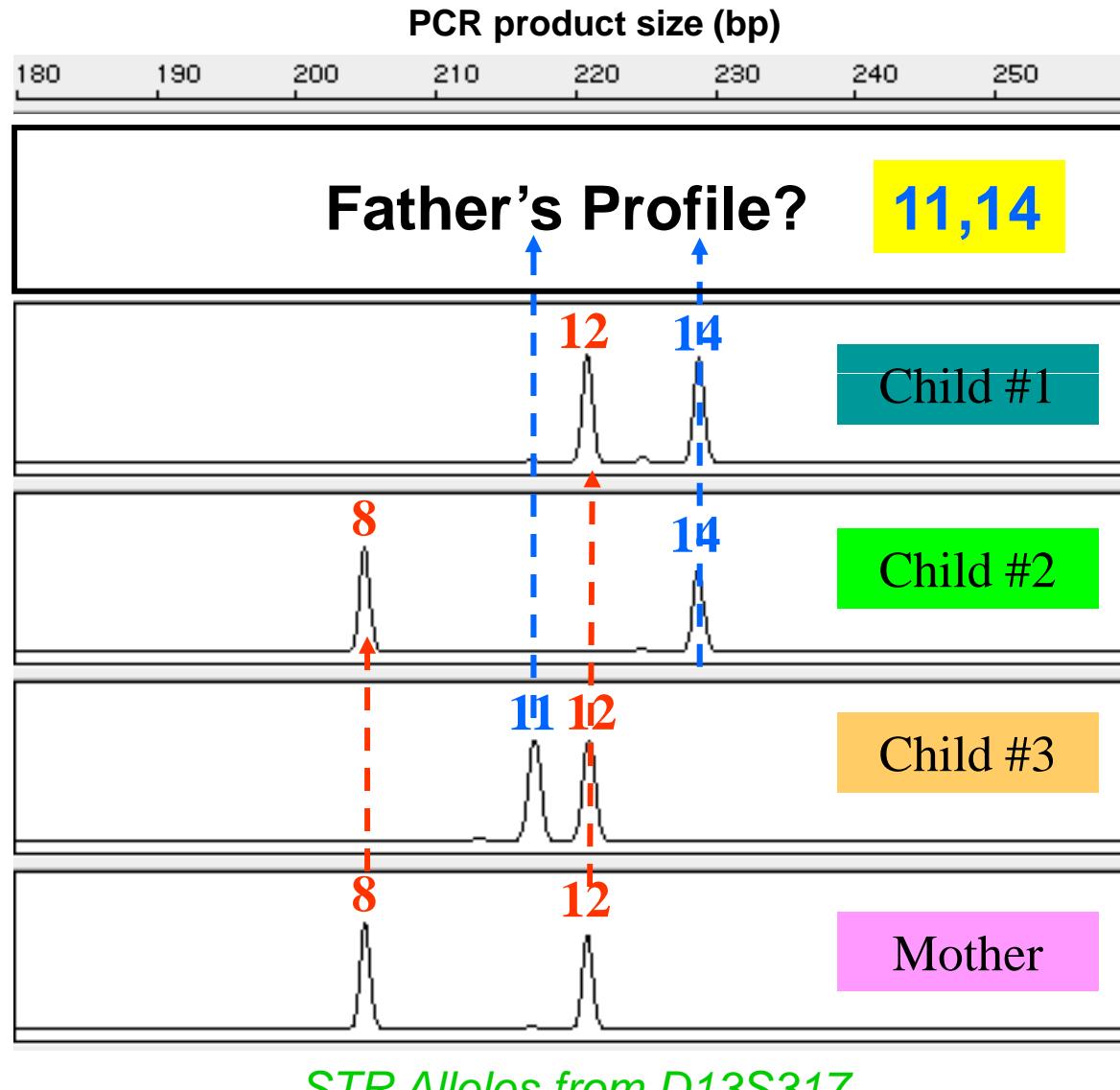
Permit Entry

Match of 13 points (each with 2 variable alleles) within DNA

String of 26 numbers (order of listing DNA results would have to be standardized)

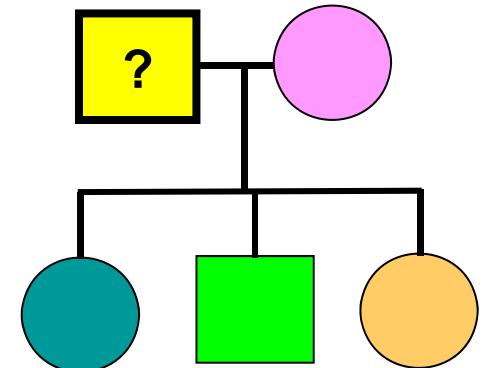
16,17-17,18-21,22-12,14-28,30-14,16-12,13-11,14-9,9-11,13-6,6-8,8-10,10

# Enrollment through Relatives



## Paternity Testing

Alleged Father(s) is asked to donate DNA sample



# NIST Efforts with DNA Biometrics

- **Developing rapid PCR protocols**
- Evaluating kinship analysis software
- Support to other rapid DNA efforts
- Designing standards materials for device testing
- Preparing to test prototype rapid DNA devices

# Current State of Rapid PCR Protocols

- Rapid amplification of at least 16 loci is possible
  - <20 minutes
- Faster DNA polymerases are required
- Faster thermal cyclers are required
- Optimized rapid STR typing kits could be produced specifically for portable integrated devices
- Success with ~1 ng of DNA template (single source)
- Sub 45 minute PCR will be essential for rapid typing in a integrated/ portable system

# ANDE (Automated Nuclear DNA Equipment)

## US Government Prototype Initiatives

### **Rapid DNA Profiling System Automated Nuclear DNA Equipment (ANDE)**

**(a joint DoD/FBI/DHS initiative)**

- Analysis and matching of multiple DNA samples in **1 hour (18 month development program)**

### **DHS Low-Cost and Rapid DNA-based Biometric Device**

- Demonstrate an automated desktop prototype device that verifies identity or kinship **within an hour (2 year development program)**

# Speed Improvements with DNA

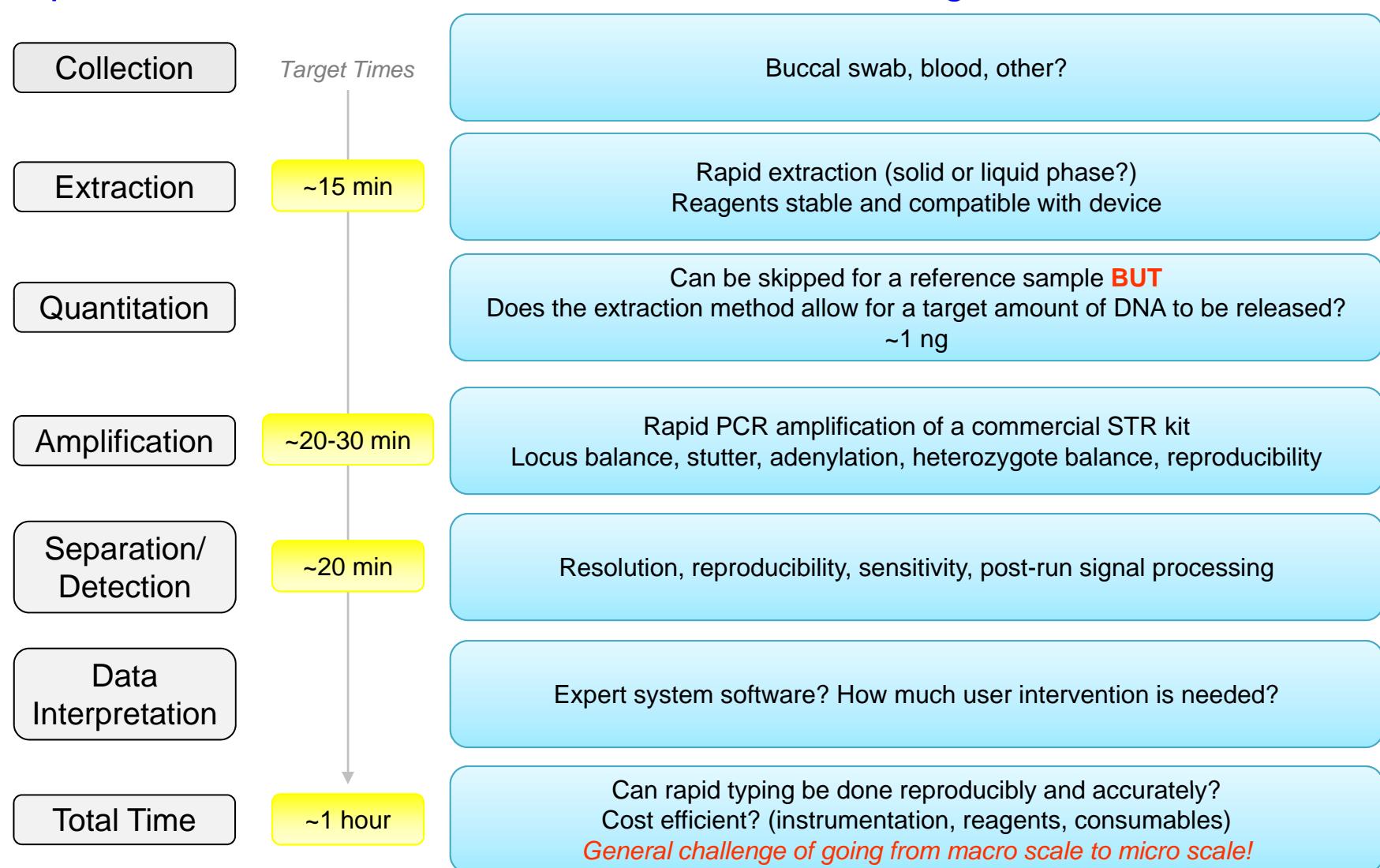
## Turnaround Time Over Last 20 Years

1988 - 94	P-32 RFLP	~ 7 weeks for 6 loci result
1995 - 96	Chemiluminescence	~ 9 days for 6 loci result
1994	PM – DQA-1 PCR	~ 3 days for 6 loci result, > Sensitivity, < Stats
1998	STR with CE	~ 3 days for 13 loci result, > Sensitivity, > Stats
1998	NDIS Established	
2006	Expert System Approved	
2009	R-DNA (R&D)	~ 4 hours for 13 loci (manual intervention)
2011	ANDE (Prototyped Plan)	~1hr 8-16 swabs @ \$100/Sample

Real time DNA analysis can lead to real time DNA ID

# DNA Analysis Approach (integrated)

## Steps Involved



## Contact Information

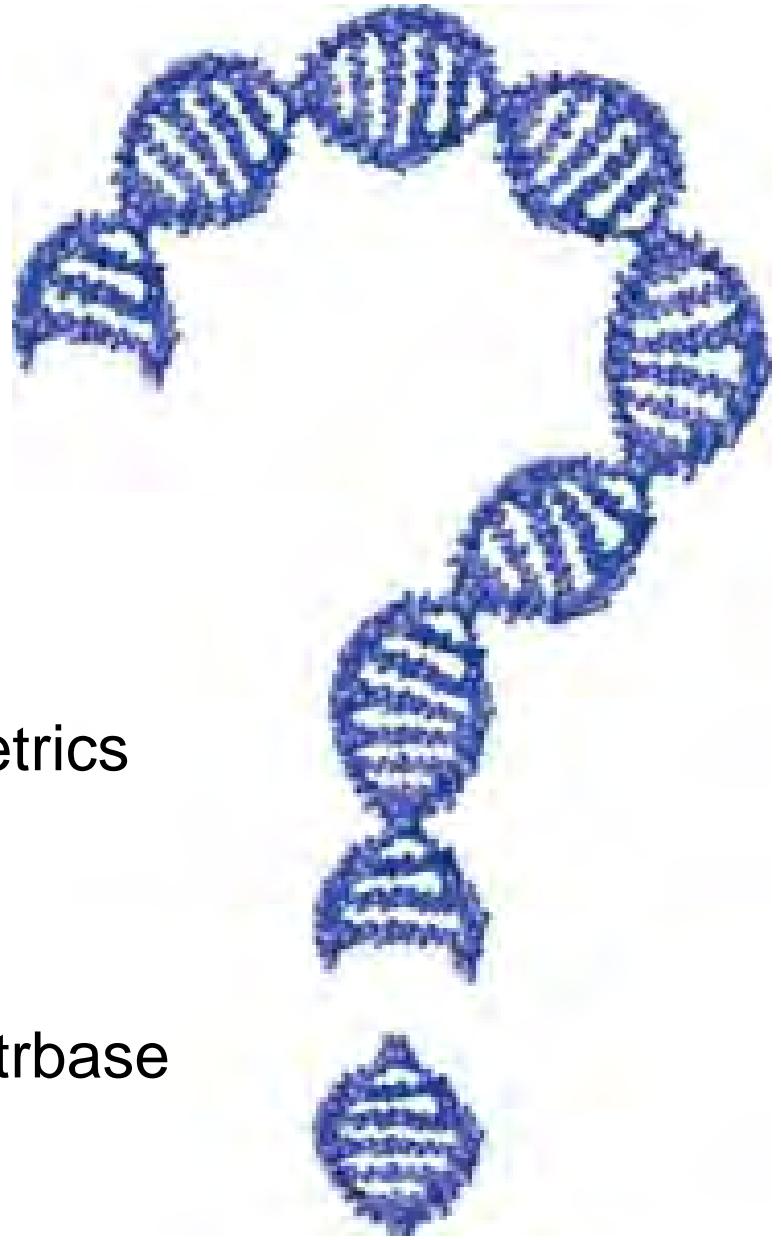
**Peter Vallone**

Project Leader, NIST DNA Biometrics

[peter.vallone@nist.gov](mailto:peter.vallone@nist.gov)

301-975-4872

<http://www.cstl.nist.gov/biotech/strbase>



# Industry Members

- All-Star Consulting, LLC
- American Systems Corporation
- AOptix Technologies, Inc.
- Aware, Inc.
- BAE Systems
- Booz Allen Hamilton
- CACI, Inc. - Federal
- Cogent Systems
- Cross Match Technologies, Inc.
- Daon, Inc.
- E.L.S. and Associates
- General Dynamics Information Technology
- Hitachi America, Ltd.
- Ideal Innovations, Inc.
- ImageWare Systems, Inc.
- INCERTO Technologies, Inc.
- Indiana State University
- Integrated Forensic Laboratories, Inc.
- International Biometric Group
- Iritech
- L-1 Identity Solutions, Inc.
- L-3 Communications GS&ES
- Lockheed Martin Corporation
- MorphoTrak
- National Interest Security Company, LLC
- NetApp
- Northrop Grumman Corporation
- Purdue University
- Raytheon Company
- SAIC
- SRA International
- StraTerra Partners
- Telos
- University of Notre Dame
- Virginia Tech
- WCC
- Smart Search and Match
- West Virginia University
- Wiser Company

# Government Members

- Biometric Task Force
- Department of Homeland Security
- Department of State Dept. of State Consular Affairs
- FBI/CJIS Division/Biometric Services Section
- Customs and Border Protection

# SmartGate



## 2010 Biometrics Conference “The link between the Battlefield & Borders”

### SmartGate and Automated Border Processing

Presented by:

Chris Dennis

Counsellor, Americas

Australian Customs and Border Protection Service

Embassy of Australia

Washington DC



# Presentation Outline



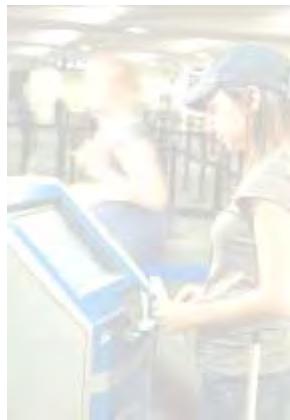
- Background
- The Challenge
- What is SmartGate?
  - How does it work?
  - Who can use it?
  - Where is it?
- An end-to-end solution
- Improving the user experience



# Background



# Customs and Border Protection Role



- Universal Visa Requirement
- Pre-arrival assessment of PNR and API
- *Face-to-passport check*
  - Where SmartGate assists.
- Alert lists
- Airport assessment via monitoring and patrols



# The Challenge



To process increasing numbers of travellers within existing floor space without comprising standards of border protection and facilitation.



# What is SmartGate?



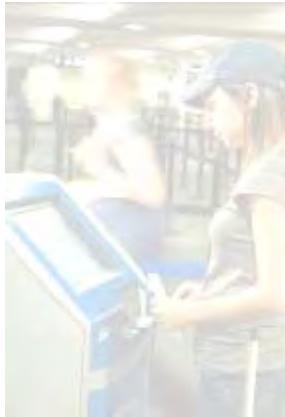
- Passport control using an ePassport and face recognition technology
  - Checks eligibility requirements
  - Matches image of traveller to image in ePassport and undertakes other checks
  - Traveller is cleared or referred to a Customs and Border Protection officer
- It is automated border processing that enables the travellers to self process through passport control



# How does SmartGate work?



Step 1: Kiosk – checks eligibility



Step 2: Gate – verifies identity and clearance



# Step 1: The Kiosk



Touch Screen



Passport Reader



Ticket Printer



PC



# Step 1: The Kiosk



Date, time, port of issue and kiosk ID



ePassport number

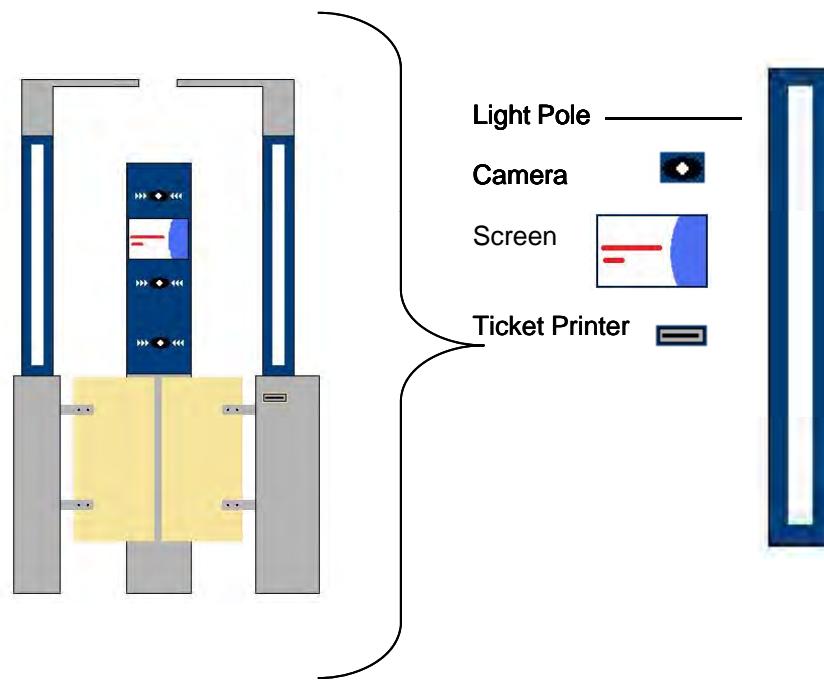
Date, time, port of issue and gate ID

Code

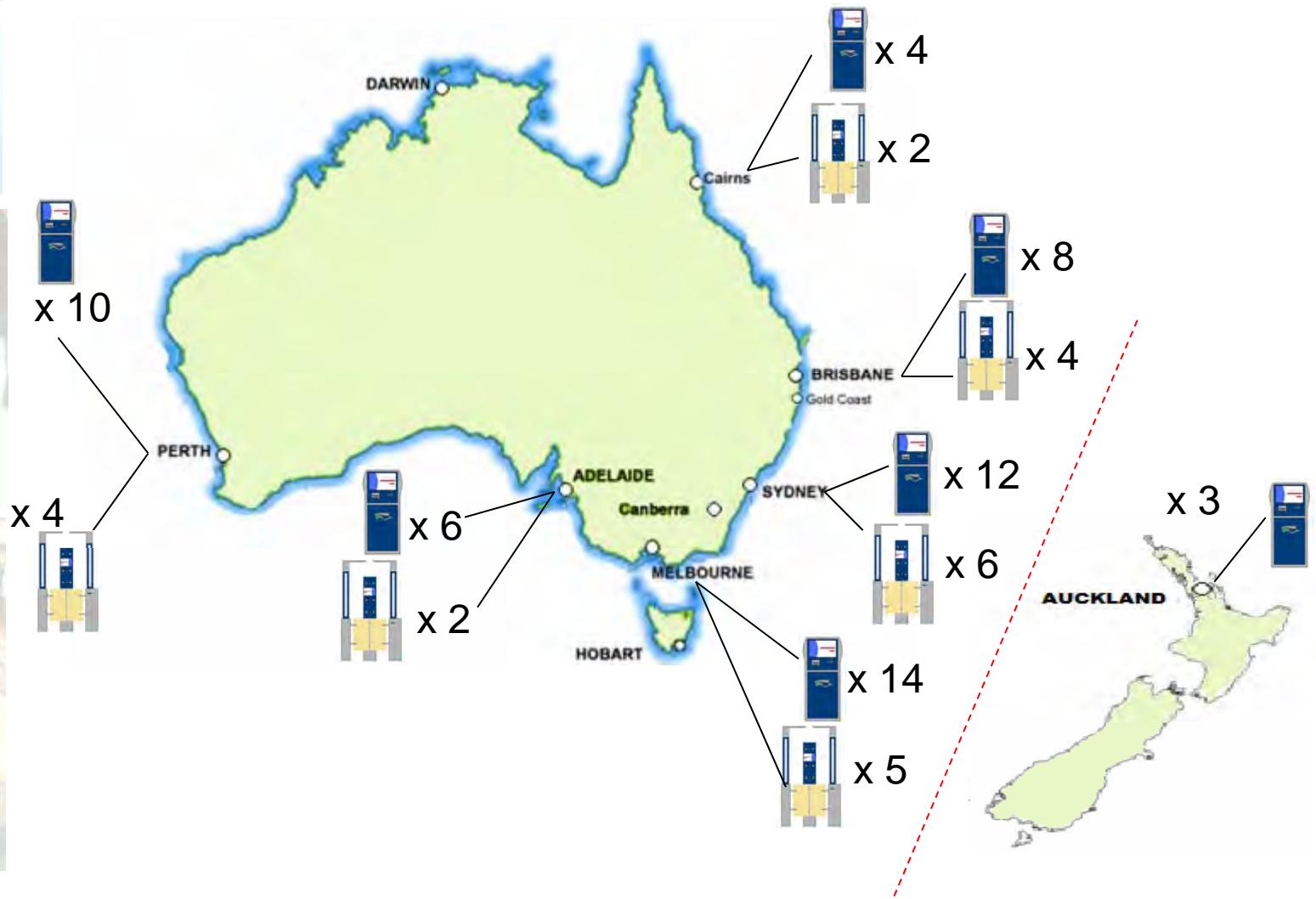
Code



# Step 2: The Gate



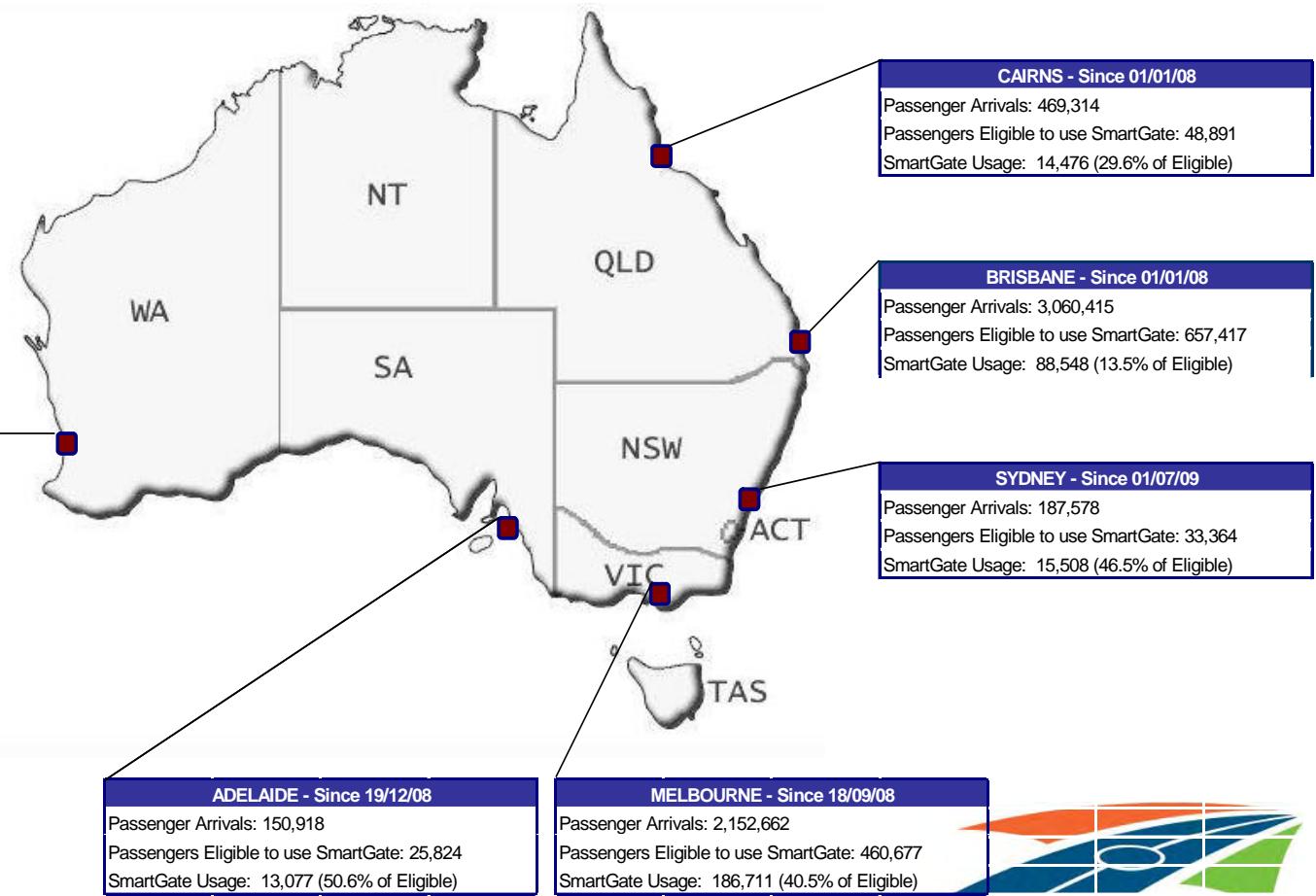
# Where is it?



# SmartGate usage



## SMARTGATE USAGE TO DATE



# End-to-end business solution



- Biometrics not used in isolation
- An end-to-end business solution
- Streamlining the passenger pathway



# Other Issues



- Privacy
- The Traveller Experience
- Relationships with New Zealand



# Where to from here?



# Questions / Discussion



# BIOMETRICS TECHNOLOGY & STANDARDS: COMMENTS ON BIOMETRIC FUSION AND IRIS BIOMETRICS

Patrick J. Flynn, Ph.D.  
Professor of Computer Science & Engineering  
University of Notre Dame  
[flynn@nd.edu](mailto:flynn@nd.edu)

# Outline

- Context
- Biometric fusion
  - Motivation
  - Definitions
  - Levels and strategies
- Advances in iris biometrics
- Summary

# Context

- Beware: this is an academic's view
- Some real success stories for biometrics
  - deployments
  - broadening familiarity
  - healthy discussions of privacy, etc.
  - strong series of technology evaluations

# Context (ctd.)

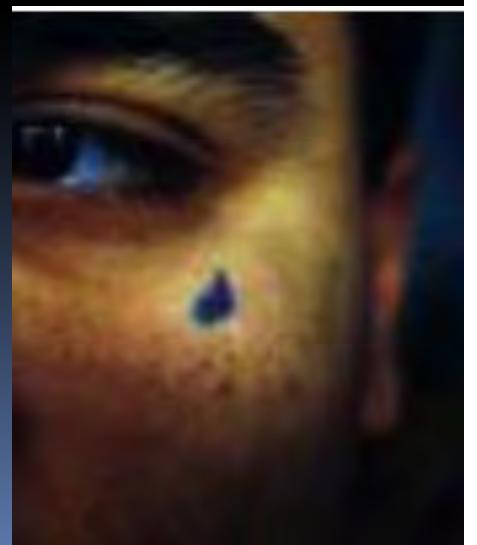
- Some challenges
  - No national-scale deployments or conversions (plans yes, deployments no; controversies, etc.)
  - Thus, many “local” decisions about technologies and systems
  - Unclear what (other than capture) is going on in some deployments
  - A LOT of ongoing debate about “who’s best”, “who’s fastest”, etc.
  - R&D resourcing landscape is... complex

# Motivating biometric fusion

- FTA/FTE circumstances
  - Iris: aniridia, strabismus, nystagmus, albinism
  - Finger: acid burns, mechanical wear (masonry)
  - Face: missing features, detection errors, cultural constraints
  - Other technology problems (lighting, power, heat, dust, lack of maintenance, etc.)

# Motivating biometric fusion (ctd.)

- Biometric traits are assumed to be “stable” – what if they’re not?
  - Face: hair growth or loss, scars/tattoos, weight gain or loss, expression variation
  - Iris: nevi, pigmentation change, ocular surgery, loss of organ, disease
  - Finger: tip distortion at time of impression



# Definitions

- Multibiometrics: many definitions
  - The **use** of multiple **samples** to improve biometric system **performance**
- Assumption: multiple samples can “cover” for one another

# Definitions (ctd.)

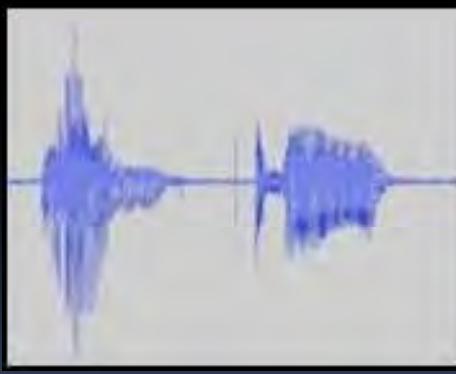
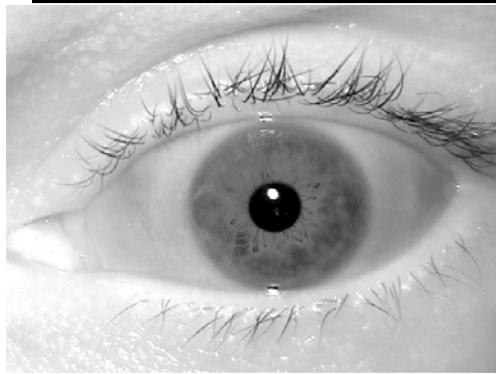
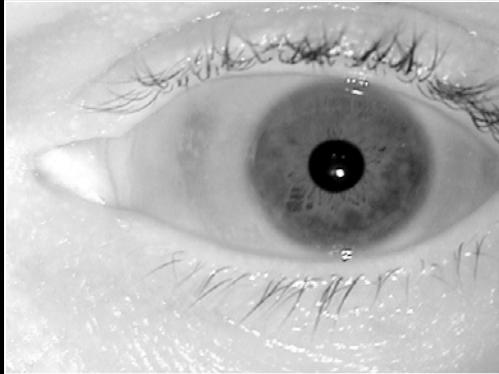
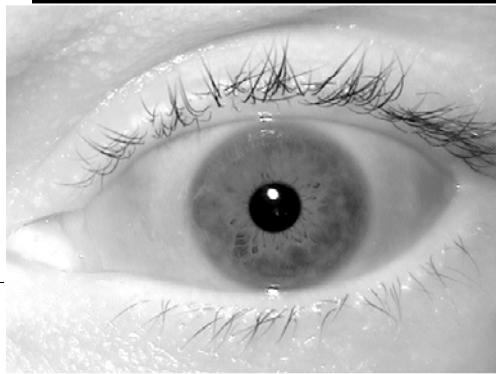
- **Samples**

- Mode (visible, IR, 3D, still/video)
- Site (face, finger, ear, palm)
- Count (1 still →  $n$  stills → video?)

- **Performance**

- Speed (matches per second)
- (preprocessing time)
- Accuracy (FAR/FRR, EER, R<sub>1</sub>R)

# Samples, sites, and modes



# Multibiometric fusion

- **Use:** you have all of these samples... And you want one decision
- Assumption: for each sample, there is a matching “box” that computes a match score from the probe sample and a gallery sample
- Fusion levels
  - Signal, feature, score, rank, decision

# Fusion: typical approaches

- Signal level: sample concatenation, e.g. pairs of face images processed as a single entity
- Feature level: construct hybrid signature from features of multiple samples
- Score level (most popular)
  - Compute a function of all scores
  - Max, min, sum, etc.
- Rank level: synthesize composite rank
  - E.g.: Borda count

# Fusion: considerations

- All matchers are not created equal
  - Characterization of performance (in typical conditions) highly useful
  - Approach broad performance claims with skepticism
- Consider cost/benefit tradeoffs prior to investment in multibiometrics
  - 2 samples of one mode/site may perform as well as one sample from each of two modes or sites... and will likely be much cheaper
  - But the future will be multibiometric (for coverage)

# Advances in iris biometrics

- Iris: a high-performing biometric trait...
  - With cooperative subjects
  - Imaged by good optics
  - Illuminated by “good lights”
- Renaissance in iris recognition research since 2004
  - Relaxation of constraints
  - Large open databases and challenge problems
  - New technologies

# Iris: Considerations

- Sample quality (improved definitions)
  - Motion blur, focus, occlusion
  - Illumination, interlace
  - pupil size, inherent contrast
- Template age (controversy)
- Video processing (not just stills)
- Liveness detection and anti-spoofing
- Spectrum (visible light instead of NIR)
- Standoff

# Iris: near future

- For procurers/deployers: possibly an increase in size of vendor space?
- For vendors: large-scale tests, constraint relaxation
- For researchers: many areas to explore
  - Headroom for improvement vs. sample sizes needed for statistical rigor

# Parting shots

- The future is multibiometric
- Iris recognition (once thought mature) may expand its footprint into less-controlled acquisition contexts
- Impact on standards?
- Uptake speed?



# BIOMETRICS TASK FORCE

**VISION FOR THE FUTURE**

***The Biometric Link – Connecting the Dots***

**Dr. Myra Gray, Director**

**20 January 2010**



**BIOMETRICS**  
TASK FORCE





BIOMETRICS  
TASK FORCE

practices  
tests

defense

\$100

united  
federal  
attacks



## Example #1: Hoax IED





## Example #2: Atlanta Airport



# Example #3: Swar Khan

Swar Khan - Wikipedia, the free encyclopedia - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back   Search  Favorites    Go

Address  [http://en.wikipedia.org/wiki/Swar\\_Khan](http://en.wikipedia.org/wiki/Swar_Khan)

Help us provide free content to the world by [donating today!](#)

article discussion edit this page history

Log in / create account

**Swar Khan**

From Wikipedia, the free encyclopedia

**Swar Khan** (born c. 1970) is a citizen of Afghanistan, held in extrajudicial detention in the United States's Guantanamo Bay detention camps, in Cuba.<sup>[1]</sup> His Guantanamo Internee Security Number is 933. American intelligence analysts estimate Swar Khan was born in 1970, in Khost, Afghanistan.

Swar Khan was a security official for the Hamid Karzai government prior to his capture.<sup>[2]</sup> His boss told reporters that his capture was due to false denunciations from a jealous rival, whose sons worked as interpreters for the Americans, and that he had tried to tell the Americans he should be set free -- without success.



Do you own one?

[, please click here](#)

1970 (age 38–39)  
Khost  
2006-10-11  
Afghanistan  
Afghanistan  
Guantanamo

Initially the Bush administration asserted that they could withhold all the protections of the Geneva



## Example #4: Fairfax County Police Dept.





# Current DoD Business Function Applications





# Facility Access





# Physical Access





# Information Verification





# Eglin Air Force Base



**U.S. AIR FORCE**  
**Eglin Air Force Base**

A large, illuminated sign on a brick building. The sign features the U.S. Air Force symbol (a stylized eagle with wings spread) above the text "U.S. AIR FORCE" and "Eglin Air Force Base". The sign is set against a background of a brick wall and a blue sky with a circular emblem in the upper right corner.



**BIOMETRICS**  
TASK FORCE





BIOMETRICS  
TASK FORCE





Keynote Remarks Given by Dr. Myra Gray

NDIA 2010 Conference

January 20, 2010

**FINAL**

## **VISION FOR THE FUTURE**

### **THE BIOMETRIC LINK – CONNECTING THE DOTS**

#### **Keynote Address (30 minutes)**

[Title slide #1]

Ladies and Gentlemen, Welcome to the National Defense Industrial Association (NDIA). I am honored to be your Keynote Speaker today. For those of you who have come from outside the Washington, DC metro area, we're especially pleased to have you join us today.

**Attacks of terror happen every day around the world.**

- They happen in far away Iraqi battle zones.
- They happen in remote Afghan villages infiltrated by the Taliban.
- They happen in crowded cities and bustling markets.

- They happen in international waters...on US soil...and in well-traveled airspace – the latest of which we saw on Christmas Day.

No one is immune. All we can do is work hard to prepare and protect ourselves and our country using the best resources, people and technology available. And we must demonstrate a sincere and determined attempt to stay one step ahead of the terrorists.

In the aftermath of the Christmas Day attempted bombing of yet another commercial passenger jet, President Obama noted that “we” -- referring to all aspects of the federal government – *failed* to “connect the dots” to identify and stop this attempted terrorist attack before it occurred.

[DOTs slide #2]

And he’s right. Whether you call them dots or silos, a narrow view of the importance of our individual missions will not take us where we need to go. We must work

together – both within government and across government, industry and academia – to create and manifest a broad and successful strategy to defeat terrorism as we know it.

So just what are the “dots” in today’s challenging environment and how can we connect them in the most efficient manner to ensure this kind of attack – and other types not yet witnessed – don’t occur again?

In our day-to-day work in DoD biometrics, the “dots” include everything from data collection and analysis to storage and matching. They are also the individual soldiers, sailors, airmen and marines who collect biometrics as part of their jobs. They are the examiners who strain to interpret the minutia of a latent fingerprint. They are the scientists and engineers who look long into the future to visualize and create better, cheaper and faster systems. They are the researchers and teachers whose quest for knowledge and commitment to educate others will perpetuate and expand both the science and the applications of biometrics. They are the people who

ensure that all of our multilateral and interagency agreements are in place with the T's crossed and I's dotted. They are the people who develop our specifics requirements and those who properly and effectively communicate our needs and successes to all the right people. And they are certainly representatives of industry – like you – who strive to improve current systems, expand capabilities and keep us all ahead of the terrorists.

So what does it take to connect all these “dots” into a meaningful and successful operation? It takes a lot. Putting all these dots together is like creating a great work of art – no one dot is more important than another, yet together they form a strong foundation and a beautiful picture. Not to mention the impact they are having in fighting terrorism and protecting the homefront.

Today, however, I'd like to highlight just a few of the critical components we must have in place to connect the dots. First, it takes: [Determination Slide #3](#)

Determination, dedication and a common desire to identify and take those intent on harming America and Americans out of circulation.

It also takes: [Objectivity Slide #4](#)

Objectivity and the ability to visualize the bigger picture through the implementation of a common architecture, seamless integration and the interoperability of systems and data.

Furthermore, it takes the: [Transformation Slide #5](#)

Transformation of business practices, ways of thinking, and operational patterns to create efficiencies never before imagined.

Finally, it takes: [Standards Slide #6](#)

Standards that are universally acceptable, easy-to-understand, flexible and inclusive.

And if you were really paying attention to what I just said, you might have noticed that the acronym for these four critical areas is:

D O T S. Easy to remember, huh? [\[DOTS Slide #7\]](#)

The good news is that Biometrics and the progress we at the Department of Defense and across the federal government have made in the past several years utilizing this technology and sharing the resulting data IS working. We have successfully connected disparate and seemingly insignificant bits of information and data into facts and reference points. We work with our interagency partners on a daily basis to connect and share our individual yet synergistic efforts.

And through this interagency work, the need to adopt and promulgate a holistic architecture is readily apparent. Just like the foundation of a well-built home, the building blocks we use to create and expand our data repository must be solid and consistent. Likewise, just as the construction industry adheres to strict standards and performance

expectations for materials and systems, so too does the ease-of-use and interoperability for all of us depend on creating and implementing universal standards.

Then comes your role as industry...creating, manufacturing and maintaining collection devices and data transfer systems that work within the dedicated architecture and conform to established and agreed-upon standards. Oh yes, and devices that perform faster, cost less, and are more rugged and reliable every generation. Is that too much to ask? Hopefully not, particularly when we hear about the successes we're having utilizing biometrics.

So, let me tell you about a few recent examples:

### [Hoax Slide #8]

First, on 20 March 2009, a soldier discovered what was determined to be a hoax IED device on Al Asad Air Base, Iraq. Anti-American graffiti painted on the wall included the outline of an AK-47 and a hand in the form of a fist, a

possible symbol of Hamas. Eight days later, BTF examiners identified two latent prints developed from the scene to two different individuals. The latent matches gave direction in an investigation with limited investigative leads and may facilitate the identification of persons involved in the hoax.

#### [Atlanta Airport slide #9]

Second, despite airports being the focus of stringent security measures since 9/11, on 16 March 2009 the BTF received ten-print images for an individual trying to enter the United States through the Atlanta International Airport.

The individual's biometrics were searched against DHS IDENT records resulting in a potential watch list match. Our certified latent print examiners formatted the prints for submission to the DoD ABIS confirming a Tier 5 "Deny Base Access" watch list hit. Needless to say, that individual's trip likely ended there without the benefit of frequent flyer miles.

## [Khan Slide #10]

Another dramatic example involves the case of Swar Khan. Mr. Khan has a “rap sheet” a mile long, which in biometric terms translates into many entries in the ABIS database dating back to 2003. But let me bring this case down to even more common level.

Mr. Kahn has such a long criminal history, that he has his own entry in Wikipedia. No kidding. No matter how you feel about Wikipedia as a reliable source of information, it's there. Do you have your own personal entry on Wikipedia?

In regards to Mr. Khan, the online encyclopedia states, ***“Swar Khan is a citizen of Afghanistan, held in extrajudicial detention in the United States's Guantanamo Bay detention camps, in Cuba. His Guantanamo Internee Security Number is 933. American intelligence analysts estimate Swar Khan was born in 1970, in Khost, Afghanistan. Swar Khan was a security official for the Hamid Karzai government prior to his capture. His boss***

*told reporters that his capture was due to false denunciations from a jealous rival, whose sons worked as interpreters for the Americans, and that he had tried to tell the Americans he should be set free -- without success."*

Good for us, because among the allegations noted for Mr. Khan are the following:

1. He is a member of the Taliban.
2. He is a former intelligence officer for the Taliban.
3. Mr. Khan participated in military operations against the United States and its coalition partners.
4. He had approximately six truckloads of weapons and ammunition including mortars and artillery stored in his house.
5. He was selling weapons and ammunition that were allegedly used against coalition forces.
6. The detainee swore written allegiance to the Union of Mujahadin under Commander Malem Jan Sobari, who is a Taliban guerrilla warfare leader in certain areas of Afghanistan.

Our ABIS records on Mr. Khan showed that he was first captured in January 2003 and quickly shipped off to Guantanamo Bay. He spent several years there and was released from GTMO in October 2006. Fortunately, the latest match to Mr. Khan which occurred in May 2009, should keep him off the streets. [\*\*He was detained by US Forces-Afghanistan at Regional Command East.\*\*](#)

### [Fairfax Police Slide #11]

Security needs span all facets of law enforcement and information sharing is critical. And while the work of the BTF reaches into the most remote corners of the world, it is also working literally in our backyard. The Fairfax County Police Department (FCPD) has been using digital fingerprints to identify criminals since 1984 and facial recognition technology since 2007. The FCPD operates the National Capital Region (NCR) Automated Fingerprint Identification System (AFIS), a fingerprint identification system connecting police departments of local cities and counties in the Washington D.C. metropolitan area. The FCPD also operates its own jurisdiction's multimodal

biometric system called the Northern Virginia Regional Identification System (NOVARIS), which is a fingerprint and facial image repository that currently contains about 500,000 files.

Those files are accessible by three counties and several separate municipalities in Northern Virginia. Data-sharing agreements are in place between the National Capital Region police departments, which are all collecting biometric data in accordance with established standards and best practices. They also conform to international standards for sharing data with INTERPOL. NCR-AFIS, which contains about 1.5 million files, was updated in 2007 to include facial imagery from arrests – or what we know as the classic “mug shot.” Recently, this facial recognition technology was successfully used by a Maryland law enforcement agency to identify a bank robbery suspect.

In addition to partnering in the testing of mobile biometric collection devices during future biometric field exercises, we hope to provide NOVARIS officials connectivity and an information-sharing arrangement between its intelligence

section and the DoD ABIS that would allow NOVARIS to search against the DoD database if NOVARIS officials suspect that they have data on someone who we might as well.

These examples are just a few of those that demonstrate:

1. Biometrics ARE working.
2. Those involved in biometrics across the federal government ARE working together.
3. And those across all sectors – government, academia and industry -- ARE collaborating and sharing critical data, important successes and a common vision for the future of biometrics.

In other words, connecting the DOTS.

### [Business Functions #12]

But in order to make biometrics ubiquitous across the federal government and our society in general, more uses need be developed and applications of the technology

expanded. Ordinary day-to-day uses of biometrics are paving the way to make biometrics an enduring capability. Some of those non-combat areas of the Department of Defense that are currently benefitting from biometrics include:

- Facility access [[Slide #13](#)]
  - Monitoring pedestrian and vehicular traffic at bases, ports and military installations
- Physical access [[Slide #14](#)]
  - Controlling secure areas and limiting cleared personnel
- Information Verification [[Slide #15](#)]
  - Providing identity confirmation to allow access to medical or employment history or speed financial transactions

### [\[Eglin AFB Slide #16\]](#)

Take for example, biometrics in use at Eglin Air Force Base in Florida. Despite having a state-of-the-art Veterans Administration Medical Clinic adjacent to the base, getting from the VA clinic to the base hospital for

additional treatment or tests was no easy task. That was especially the case for the many elderly, retired or disabled veterans living in the area. That is until a partnership between the Veterans Administration and the Air Force was formed that created a biometrically-enabled gate between the two facilities. Now, when patients come to the VA medical clinic and need additional tests, volunteers who are enrolled in the hand geometry system there can put them in a golf cart and speed them through the gate and over to the base hospital. The patient doesn't have to drive from one place to the other – or worse yet, try to find a ride and then pass through the stringent security at the main gates of Eglin.

### [Dot Slide #17]

So as you spend the next **two** days here learning more about biometrics, hearing from those inside government and those across the industry, and sharing important updates with your colleagues, I hope you will all strive to connect the dots. Or, if nothing else, I hope you will at least remember my definition of that acronym as an

inspiration for moving biometrics forward: **D**etermination,  
**O**bjectivity, **T**ransformation and **S**tandards.

[Animation of last slide]

Just like no one is immune from terrorism, no one alone can advance biometrics. We must all work together so that biometrics curtails terrorism, fortifies our security systems and just plain makes our lives easier.

Thank you.

###

# Private Sector Uses of Biometrics: From High-Stakes Testing to Loyalty Cards

---

Prepared for the

**National Defense Industrial Association  
Biometrics Conference**

January 21, 2010

**Kathy Harman-Stokes, J.D., CIPP**

U.S. & International  
Data Protection & Privacy Law

+1.703.216.5643 direct  
kathy@stokes-law.com

# Private Sector Use of Biometrics: From High-Stakes Testing to Loyalty Cards

- High-Stakes Testing: Preventing Fraud in the GMAT® Exam
- Advances in Employee Access Control, Time & Attendance Tracking
- Biometrics to Secure Data at Data Level: Protect Every Mouse Click
- Consumer Authentication/Identification
  - Biometrics in Banking
  - Biometrics at Retail Point of Sale
- Biometrics in the Hands of Consumers

## High-Stakes Testing: Preventing Fraud in the GMAT®

- Scores used by 1900+ schools in 70 countries
- Delivered in 110 countries to approximately 250,000 people annually
- 2003: 6 individuals impersonated 185 business school applicants
- Exam fraud = fraud on the schools using scores. Unethical applicant gets in, honest applicant left out
- 2006: Began biometric fingerprints
- Process:
  - First time test taker provides print at test center check-in.
  - Upon returning from break, new fingerprint compared to original, 1:1
  - If person re-tests, new print compared to original, 1:1
  - If no match, manual investigation.



## High-Stakes Testing: Preventing Fraud in the GMAT®

- Yet, technical challenge with fingerprint
- Legal challenge: Strong cultural sensitivity to fingerprints, based on Nazis, Stasi/secret police.
  - In Europe, right to privacy is “fundamental human right,” basis of civil society, democracy
  - Embedded in national constitutions, European and EU law
  - Data collection, use and transfer out of EU highly regulated
  - Overriding EU law, plus national laws, with independent data protection authorities (“DPAs”) with varying powers
  - DPAs provide check on private and public sectors
  - Fingerprints rejected by some European authorities
- 2009: Shift to Fujitsu palm vein biometric

## High-Stakes Testing: Preventing Fraud in the GMAT®

- Palm vein system designed to meet challenges:
  - 1:N matching on the horizon
  - “No trace”: User leaves no trace on device and no surreptitious collection
  - No image stored for later use
  - Unique algorithm to prevent interoperability
- July 2009: France’s authority, the “CNIL,” approved GMAT’s collection, 1:N matching, and transfer of data into central database in the US
- Most other EU countries expected to follow
- Palm vein implemented in over 100 countries



## Biometrics for Employee Access, Time, Attendance

- **Global Rainmakers:** Iris Recognition System

- High throughput while person in motion (up to 50 people/minute)
- Ex: Large US bank using for employee building/logon access
- Quick efficient system for 1:N
- Less public resistance than w/fingerprint



*Ex: Employee access through turnstiles*

- **Aurora:** Face Recognition System

- Solved lighting problem using infra-red
- Almost 100 clients, 940 sites in UK and Middle East: e.g., construction industry, colleges, airport operators using for 1:1
- Ex: Engineering company using for employee access, time/attendance, with data passed to timesheet and payroll systems
- Ex: Colleges using to track students' attendance

## Securing Data at the Data Level: bioLock

- bioLock: Only SAP certified biometric system
- Secures HR, financial, health, research and other data at the data level, mitigating fraud and ID theft
- Protect any mouse click
- Swipe fingerprint on keyboard or mouse for 1:N identification for:
  - Initial computer log on
  - To view or edit particular data, e.g., employee/customer health info, financial records
  - For standard workflow approvals, e.g., manager approval of budget
  - To authorize a transaction, e.g., authorize wire transfer



## Securing Data at the Data Level: bioLock

- Blocks access for those not authorized
- Logs every attempt, identifies anyone in the system
- Reduce or eliminate reliance on passwords, risks of phishing
- Strong solution for Sarbanes-Oxley financial controls and HIPAA compliance
- Current users of bioLock include:
  - Major EU bank, other banks
  - European and US energy companies
  - European hospitals
  - California state universities, city governments



## Biometrics for Customer Authentication/ID

- National Australia Bank: Voice Recognition

- 35 million customers. Significant losses from fraud, e.g., phishing, trojans, “man in the middle” trojans, ID theft
- 2009: launched voice recognition for phone banking
- Starting w/customers who cannot remember PIN code:
  - Previously, manual, time-consuming process. Ask 5 pre-selected questions.
  - Answers to questions now available on Facebook (e.g., high school mascot). Expansion of social networking leading to expansion of fraud, ID theft
  - Now, 85-90% of these customers enroll in voice recognition for 1:1 authentication.
- VR enrollment is manual process, repeating info for print creation

## Biometrics for Customer Authentication/ID

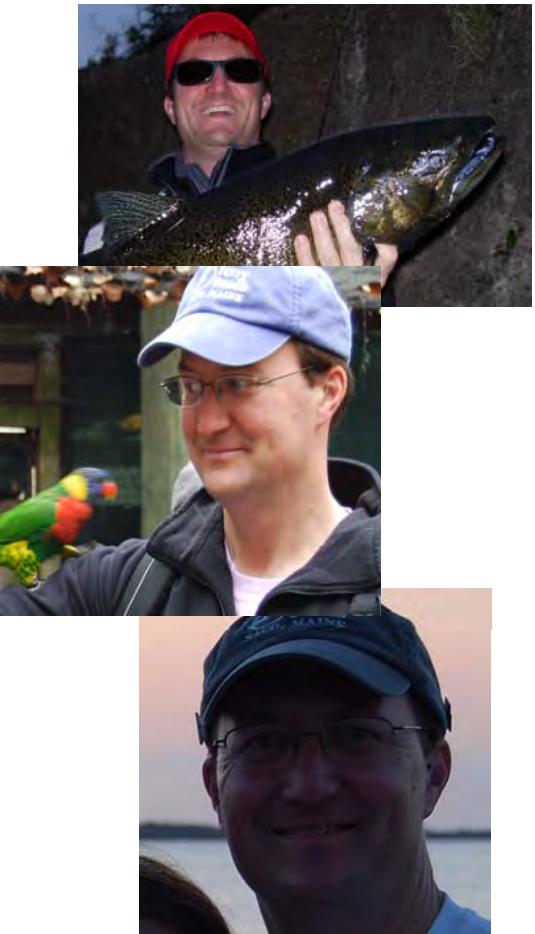
- National Australia Bank:
  - Post-enrollment, customer calls automated system: if no PIN, put into VR system
  - Customer says NAB known ID number and DOB
  - System matches what is said for accuracy: correct NAB ID and DOB?
  - And matches whether voice print matches that NAB ID and DOB
  - 50K enrolled customers; exploring offering to all customers
  - Better customer experience than 5 questions; saves staff time/costs
  - With other security improvements, substantial reduction in fraud losses
- Several Japanese Banks: Palm Vein on ATMs

## Biometrics for Customer Authentication/ID

- EasySecure, Netherlands: Fingerprints at Retail Point of Sale
  - Fingerprint system authenticates customers, allows access, charges to account or as loyalty card
  - Manual enrollment process, web-based application
  - Allows 1:1 or 1:N matching
  - Post-enrollment, customer scans fingerprint, system checks against central database to authenticate or identify, approves or denies
  - Ex: At fitness centers, swimming pools, fingerprint allows access according to subscription
  - Ex: Camping store sets up customer account tied to fingerprint; allows charges via fingerprint from family
  - Ex: As loyalty card, fingerprint tracks purchases or points
  - No image retained; image retention generally now allowed in NL or Belgium

# Biometrics in the Hands of Consumers: Face Recognition Applied to Photos

- Apple® iPhoto® “Faces,” Adobe® PhotoShop®, other photo-sharing web sites group photos by faces
- Consumer’s photos added to photo site
- Site software applies FR biometric technology to all photos, grouping together photos of people with the same faces
- Consumer adds names to each group of faces
- Convenient tool for consumers – easy to create albums for friends, family
- Possibly millions of biometric FR templates stored on web-servers through sites



## Conclusion

- Biometric use spreading rapidly in private sector – employees, and also retail and consumer applications
- Increased convenience, more accurate information, reduces employer admin costs
- But, what recourse if biometric data/ID stolen? How is data being used, by whom?
- Privacy and legal questions: In the US, not aware of any specific oversight or laws that apply to biometrics (except Illinois)
- Europe and US legal regimes share several common goals: fully inform consumers, give them choices, abide by their choices
- Europe: Strong rules and limits around biometric data use
- US: Goals met sporadically, case by case. Some disclosure and choice, determined by company. Do consumers fully understand? Limits on biometric use?
- As growth continues, when a major problem arises, regulation likely

### Kathy Harman-Stokes, J.D., Certified Information Privacy Professional

Kathy is an attorney and consultant on US and international data privacy laws, advising a broad range of clients on privacy laws, focusing on biometric laws. She advises her clients on, among other things, legal issues arising from the use of biometrics in specific countries, how systems should be designed to comply with international laws and where and how biometric data may be transferred. For 6 years, she was the Associate General Counsel and a corporate officer at the company that owns the GMAT exam, a high stakes test used for graduate business school admission worldwide. Kathy oversaw legal compliance efforts for the GMAT's collection of fingerprints and palm vein biometric data in 110 countries, and held discussions with EU data protection authorities concerning biometrics and other sensitive data. Before her work with the GMAT, she was an attorney at Hogan & Hartson LLP in Washington DC and McLean Virginia, specializing in litigation, employment and intellectual property matters. She attended the University of Virginia School of Law, and is an IAPP Certified Information Privacy Professional\*.

*\*The Virginia State Bar has no procedure for approving certifying organizations.*

Apple® and iPhoto® are registered trademarks of Apple, Inc. Adobe® and Photoshop® are registered trademarks of Adobe Systems Incorporated. GMAT® and the Graduate Management Admission Council® are registered trademarks of the Graduate Management Admission Council®.

# The Link Between Battlefields & Borders

# Terrorists intent...



Bring the  
battle here



# USA Critical Infrastructure

- 1,912,000 farms
- 1,800 water reservoirs
- 1,00 municipal waste water facilities
- 5,800 registered hospitals
- 87,000 emergency service entities
- 2 billion miles of telecomm cable
- 2,800 electric power plants
- 104 commercial nuclear power plants
- 300,000 oil and natural gas sites
- 5,000 public airports
- 120,000 miles of railroads
- 590,000 highway bridges
- 2,000,000 miles of pipelines
- 500 urban public transit systems
- 26,600 banks and financial institutions
- 66,000 chemical plants
- 80,000 dams
- 3,000 federal government facilities
- 460 sky scrapers

# HSPD-24



# HSPD-24 Challenges: Unanticipated Consequences

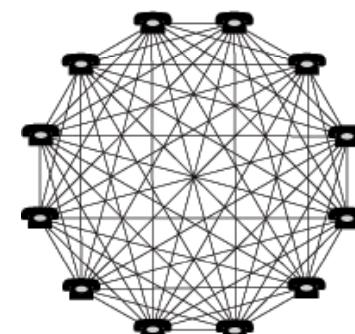
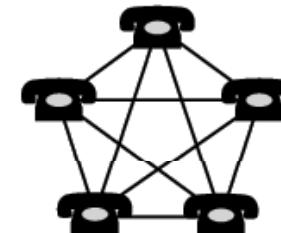
- Networks of Networks
- Quantum leaps of technologies vs procurement
- Civil Law Enforcement jurisdictions
- Civilian adoption of biometrics for identity, physical and financial security
- Emerging Social/Legal Concepts
  - Deny Malicious Anonymity
  - Insure Privacy
  - Protect Rights

# A Biometric Network

A Single Network of  
Point to Point

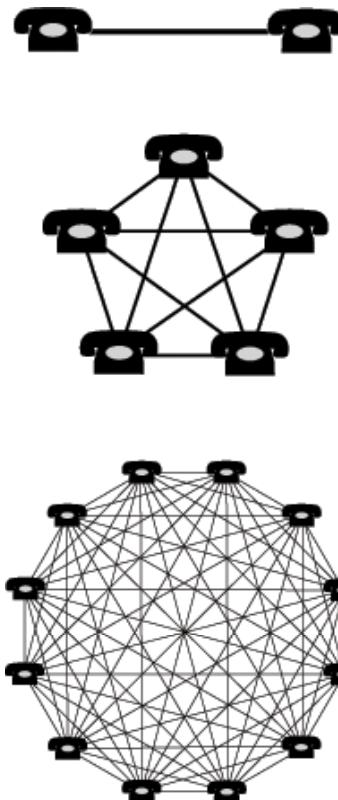
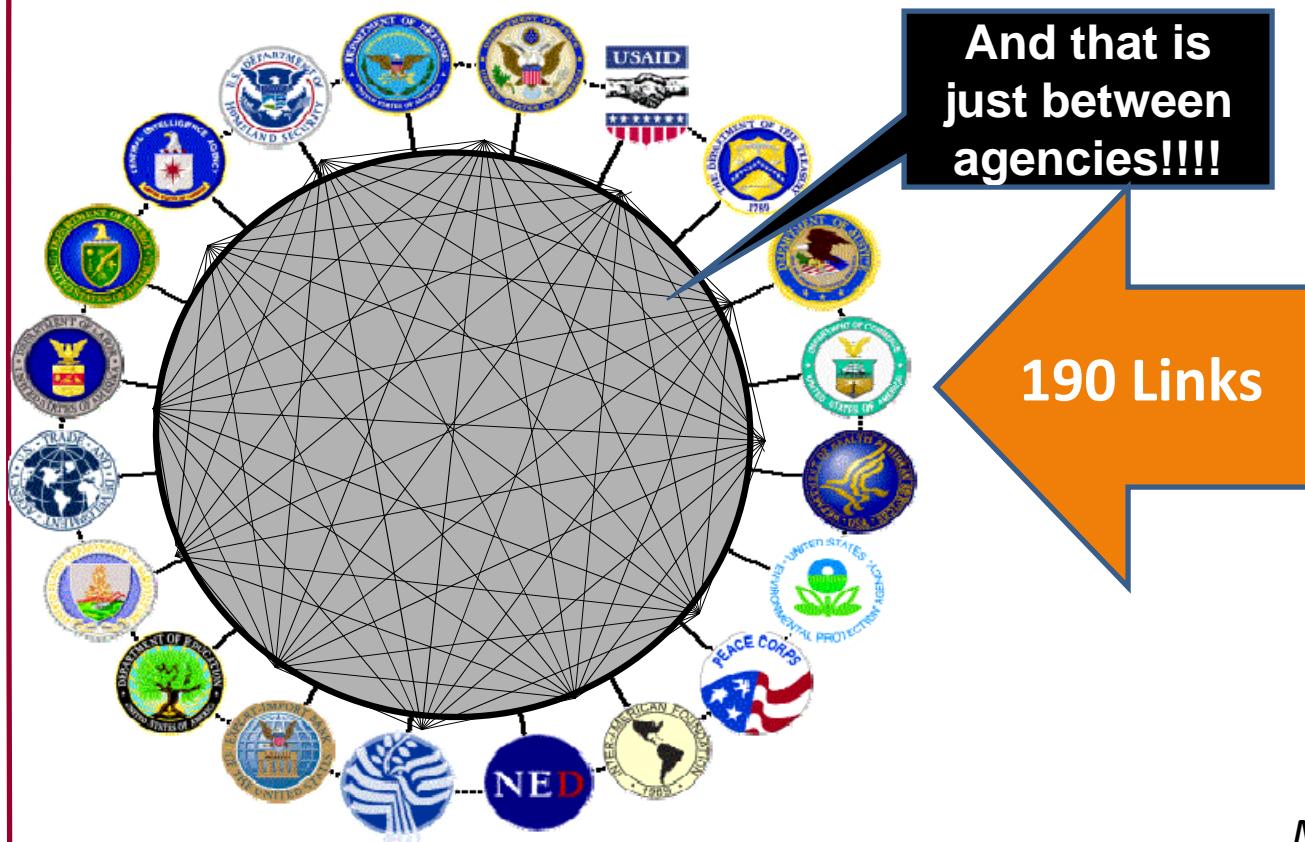


*Metcalfe Law:*  
 $n(n - 1)/2$



6

# HSPD-24: A Network of Networks



*Metcalf Law:  $n(n - 1)/2$*

# Technology Leaps, Bureaucratic Procurement Lags

- **Moore's Law:** "...processing speed, memory capacity, even the resolution of LCD screens and digital cameras (are) doubling approximately every two years"
- **US Government Procurement: Planning Programming Budgeting & Execution System (PPBS)** "PPBS imposed financial discipline, integrated the information necessary to develop effective programs to address existing and emerging needs, and established a disciplined review and approval process. However, DoD's processes for strategic planning, identifying needs for military capabilities, developing and acquiring systems, and developing programs and budgets continued to exist as disparate systems. The strategic planning process did not explicitly drive the identification of needs for military capabilities. Also, the program and budget development processes, while imposing fiscal discipline, often have failed to integrate strategic decisions into a coherent defense program. In addition, more time was being spent on deciding how much to spend on a program rather than evaluating what was received for the investment. In 2003, Defense Planning Guidance (DPG) tasked the Senior Executive Council to lead a study and identify improvements that could be made to DoD decision-making and budgeting process. Known as the DPG 20 Streamlining Decision Process, the study recommended a process that became known as Planning, Programming, Budgeting, and Execution (PPBE). Concurrent with the new planning, programming, and budgeting processes, PPBE set forth a two-year budget cycle, which allows DoD to formulate two-year budgets and use the Off-Budget year to focus on budget execution and evaluate program performance. PPBE provides a vehicle for decision makers to examine and analyze decisions by taking into consideration influencing environmental factors such as threats, political and economic climates, technological developments, and resource availability. The processes within PPBE are based on and are consistent with the objectives, policies, priorities, and strategies derived from National Security Decision directives, and shift DoD's focus from straight financial discipline to increased attention and emphasis on program performance and results. ([Office of OSD, web site](#))

## Different Perspectives

**Moore's Law** ~ 18-24 months; focuses on better and better technology;  
**“bids up” technology**

**USGov/PPBS** ~ 3-5 years; focuses on lowest cost for requirements;  
**“bids down” costs**

# Civilian Adoption

- E-Verify
- Social Security proposal
- Smart card based healthcare identity management
- RFID-enabled driver's license prove popular in Michigan

# Civil Law Enforcement

- An implied task in HSPD-24
- Hundreds of Thousands of civil law jurisdictions can provide final line of defense from Battlefields to Borders
- **Achilles Heel?** Dallas, Texas, terrorist was arrested by county sheriff's department. He said he was a foreign student. No drivers license, no insurance. Released with \$500 fine.
  - Did sheriff's have biometric technology? Did sheriff's have procedure to check against Federal data bases? Can Federal data bases take the inquiry?

# Emerging Legal & Social Concepts

- Deny Malicious Anonymity
- Insure Privacy
- Protect Rights

# Biometrics Today

© Original Artist  
Reproduction rights obtainable from  
[www.CartoonStock.com](http://www.CartoonStock.com)



search ID: grin64

"> ONLY DO BIOMETRIC READINGS NOW <"

# Welcome to the NDIA Biometrics Conference 2010

(\*We'll Need a Bigger Boat)



e-volving  
since 1949



Implementation of Biometrics and  
Single Sign-On for Access to  
Electronic Health Records

Nick Ivon

Clark & Daughtry Medical Group, PA

# Who We Are

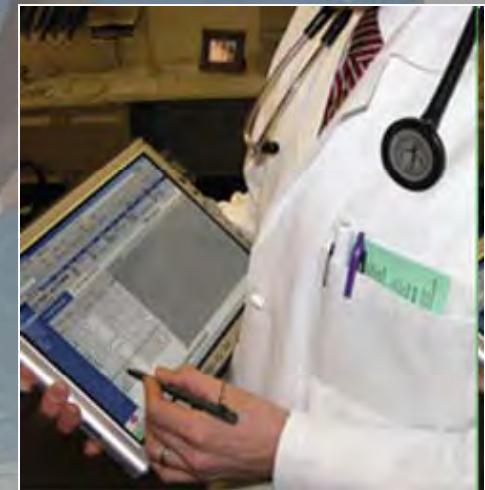
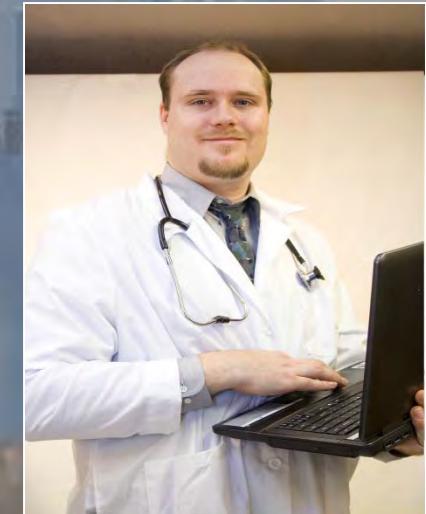
Clark & Daughtrey Medical Group, a midsize multi-specialty, multi-location provider group in Lakeland Florida, is celebrating it's 60th anniversary this month. Over the past eight years, C&D has invested heavily in technology and EMR. Our network infrastructure has been completely rebuilt from the ground up.



Clark & Daughtrey Medical

# Full EMR

Over the past three years we have transitioned all our providers to 'point-of-care', meaning each visit is electronically documented during the patient encounter. This means no paper charts, and minimal transcription services. C&D has realized a net savings of over \$500k due to these achievements.



# Small I.T. Department

We have four people in our I.T. department that manage our entire technology infrastructure, from firewalls, routers, and wireless network, to servers, PBX/IP telephony, over 400 workstations, 100 tablets, for all 7 locations. We are currently virtualizing our datacenter with VMware vSphere 4.



“Wilber is probably taking this Cloud computing too seriously.

# Use Smart Technologies

To keep our I.T. department small, we use technologies to help us manage our environment. Novell ZENworks is one tool we use to manage our servers, workstations, automate application installations and updates, and apply consistent policies throughout our organization.

A major problem was all the different user credentials for all the different systems we have to access. We needed a smart way to manage all the user logins to all the different systems.

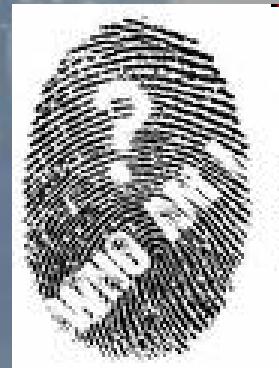


# Biometric / Single Sign-On

## A Powerful Combination

### The Problem:

- Over 25 different applications users must log into.
- Cannot control credentialing policy for most apps.
- More and more use of outside systems and extranets – makes password management even more difficult.
- Dozens of user id/password help desk tickets every week.

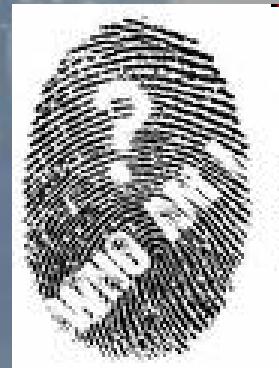


# Biometric / Single Sign-On

## A Powerful Combination

### The Solution:

- Combines biometric network authentication with Novell SecureLogin for single sign-on.
- Encapsulates user/password intelligence into the network.
- Automates application login.
- Supports workstation sharing by employees.
- Supports HIPAA regulatory requirements.
- It Actually Works!



# Solutions biometric

IdentifiPhi (now Imprivata):

The IdentifiPhi biometric solution, which includes the SAFsolution product line and BIO-key technology, allowed the use of different fingerprint readers from different vendors with one stored fingerprint.

We register users on desktops with SecuGen fingerprint readers, and these same users can biometrically login to a Fujitsu or Motion Computing notebook that uses a different fingerprint reader (usually Authentec or UPEK for portables).



# Solutions

## single sign-on

### Novell SecureLogin:

- Integrates with Microsoft AD, Novell eDirectory or other LDAP directories for application management.
- Delivers the same SSO experience in both on-line and off-line modes.
- Works with Windows apps, Internet browsers, Java, and Terminal Emulation sessions.
- Uses 168-bit triple DES or AES encryption to secure passwords during transmission and storage.
- Supports smart cards, proximity cards and tokens in addition to biometric devices.
- Supports shared workstations and fast user switching.
- Considered an industry-leading ESSO technology by [Gartner, Inc.](#)
- Built-in SNMP monitoring, allowing administrators to track events such as application logins and performance measurements (e.g., how long did it take a user to log into an application)

# Benefits of Biometric Authentication & Single Sign-On

- Virtually Password Free
- Drastically reduced number of password-related help desk tickets.
- Can re-verify biometric authentication when launching applications or any identified window or event.
- Dramatically increases security.
- Centralized administration with network directory integration.

# Bio Re-Verify Identity

```
#=====
#   =
# EXE/URL:      lrmc.netavillo.com
#=====
#   =
GetURL ?URL

#=====
#   =
# Initial Login and Invalid Login
#=====
#   =
If "preauth/login.cgi" -in ?URL
  AAVerify ?Result
  If ?Result Eq "True"
    SetPrompt "Username: "
    Type $Username #1
    SetPrompt "Password: "
    Type $Password #2
    SetPrompt "Please enter your LRMC Physicians Access information."
  EndIf
EndIf
```

Clark & Daughtry Medical Group, P.A.

# Automate Processes and automatically Notify I.S. of Events for Proactive Action

```
#####
# Name: Identiphi/SAFmodule automation
# Type: Windows
#####

#####
# Handle error window - Enrollment Failed or Cancelled
#####

Dialog
  Title "SAFmodule: Fast Enroll - Error"
  Class "TSafMessageForm"
EndDialog

Type \Alt+O
KillApp "FastEnroll.exe"
KillApp "CDBioEnrollHelper.exe"
Run "C:\Program Files\SAFLINK Corporation\FastEnroll\SendUserAbortEnrollError.exe"
Run "C:\Program Files\Novell\Desktop Automation Services>ShowAllItemsOnDesktop.exe"

#####

# Handle error window - Biometric Not Found
#####

Dialog
  Title "Error - SAFmodule"
  Class "TSafMessageForm"
EndDialog

Run "C:\Program Files\SAFLINK Corporation\FastEnroll\SendNoReaderEmailError.exe"
```

Additional tools like Auto-IT can help automate and complete the entire management process.

Almost any window or event can be identified, allowing the creation of an appropriate response.

Here we are identifying error windows and sending e-mail notifications to the I.T. department.

# Simple Example of Self Healing Application

Dialog

Title "Misys EMR"

Class "#32770"

Ctrl #2 "OK"

Ctrl #20

Ctrl #65535 "Cannot locate ifx1 service/tcp service in /etc/services."

EndDialog

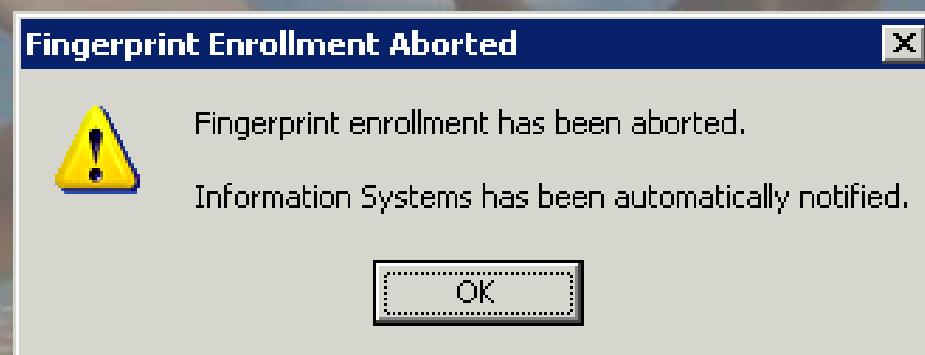
Run c:\windows\regedit.exe "/s"

"\\zenserver\sys\PUBLIC\Zenapps\EMR8\SetIfxFix\IFXfix.reg"

Click #2

# Conclusion

- Corporate environment is more secure.
- Superior desktop and application management.
- I.T. can be proactive instead of reactive.
- Fast ROI.
- Keeps us HIPAA compliant.
- Lays the foundation to deploy other identity management technologies (like provisioning) in the future.
- Life isn't good, it's great!





# Privacy Issues Associated with Biometrics

Samuel P. Jenkins, Director  
Defense Privacy Office, Department of Defense  
2010 NDIA Biometrics Conference  
January 20-21, 2010



# Focus of Today's Presentation



- Fair Information Practices and Principles
- Biometrics and Privacy Best Practices
  - Scope and Capabilities
  - Data Protection
  - User Control of Personal Data
  - Disclosure, Auditing, Accountability, and Oversight



# Fair Information Practice Principles



- Transparency – Agencies should provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).
- Individual Participation – Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Agencies should also provide mechanisms for appropriate access, correction, and redress regarding an agency's use of PII.
- Purpose Specification – Agencies should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
- Data Minimization – Agencies should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose.



# Fair Information Practice Principles



- Use Limitation – Agencies should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the agency should be for a purpose compatible with the purpose for which the PII was collected.
- Data Quality and Integrity – Agencies should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
- Security – Agencies should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- Accountability and Auditing – Agencies should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.



# Biometrics & Privacy Best Practices



## Scope and Capabilities

- **Scope Limitation**
- **Establishment of a Universal Unique Identifier**
- **Limited Storage of Biometric Information**
- **Evaluation of Potential System Capabilities**
- **Collection or Storage of Extraneous Information**
- **Storage of Original Biometric Data**



# Biometrics & Privacy Best Practices



## Data Protection

- **Protection of Biometric Information**
- **Protection of Post-Match Decisions**
- **Limited System Access**
- **Segregation of Biometric Information**
- **System Termination**



# Biometrics & Privacy Best Practices



## User Control of Personal Data

- Ability to "Unenroll"
- Correction of and Access to Biometric-Related Information
- Anonymous Enrollment



# Biometrics & Privacy Best Practices



## Disclosure, Auditing, Accountability and Oversight

- **Third Party Accountability, Audit, and Oversight**
- **Full Disclosure of Audit Data**
- **System Purpose Disclosure**
- **Enrollment Disclosure**
- **Matching Disclosure**
- **Use of Biometric Information Disclosure**



# Biometrics & Privacy Best Practices



## **Disclosure, Auditing, Accountability and Oversight (Cont.)**

- **Disclosure of Optional/Mandatory Enrollment**
- **Disclosure of Individuals and Entities Responsible for System Operation and Oversight**
- **Disclosure of Enrollment, Verification and Identification Processes**
- **Disclosure of Biometric Information Protection and System Protection**
- **Fallback Disclosure**



# Questions



# **CANADIAN FORCES DEFENCE GEOSPATIAL INTELLIGENCE**



*Predict the Environment  
Interpret the Battle Space  
Shape Operations*

# NDIA Biometrics Conference

## The link between

The Battlefield



*Foundation*



*Integration*



*Fusion*

The Borders



UNCLASSIFIED

# Canadian Military Biometrics Effort “On the Battlefield”

Mr. Yves Levesque (D GEO Int)  
[Yves.levesque@forces.gc.ca](mailto:Yves.levesque@forces.gc.ca)  
613-995-4478



*Foundation*



*Integration*



*Fusion*

# Agenda

- Introductions & Focus Area
- Afghan & Naval Collection
- Other Activities
- Future Capability
- Bridging The Gap



*Foundation*



*Integration*



*Fusion*

# Focus Area

- Military Organization
  - Military Mandate Only
  - Overseas Operational Security Requirements
  - Counter-Terrorism Mandate Only
  - Non-Canadian Data
  - Physical Security & Troop's Safety
  - Increase Identity Superiority



*Foundation*



*Integration*



*Fusion*

# Afghanistan Collection

- Policy and legal issues resolved
- Chief of Defence Staff Directive
- No Biometrics Storage Required
- No collection from Canadians Citizens
- Mandated Caveat required for ABIS upload



*Foundation*



*Integration*



*Fusion*

## Canadian Caveat

“Canadian inputted biometric data is to be used in a manner consistent with the ISAF mandate and may be shared for purposes of furthering the ISAF mandate. Any nation that wishes to use or share Canadian inputted data for a different purpose must first obtain the permission of Canadian authorities”.



*Foundation*



*Integration*



*Fusion*

# Level II Lab

- Forensic Exploitation
  - Documents Exploitation
  - Debris Collection & Analysis
  - Multi-Modal Biometrics Analysis
  - Report Drafting
- Allied Cooperation
  - Sharing Collected & Raw Data
  - Sharing Biometrics Enabled Intelligence (BEI) Reports



*Foundation*



*Integration*



*Fusion*

## Phase II

- Refining Afghan Biometrics Collection
- Biometrics at Sea Capability
  - Boarding Operations Support System (BOSS)
  - Counter-Terrorism Only
  - **NO** Counter-Piracy



*Foundation*



*Integration*



*Fusion*

# BOSS Mk III

- Computer (Toughbook)
- GPS Receiver
- Passport Reader
- Fingerprint Scanner
- Iris scanner (External)
- Wireless WiFi Camera
- Microwave Radio
- Antenna



*Foundation*



*Integration*



*Fusion*



*Foundation*



*Integration*



*Fusion*

## Other Biometrics Initiatives

- Digitize Detainees Fingerprint Cards
- Upload Legacy Data To ABIS



*Foundation*



*Integration*



*Fusion*

# Future

- Develop Enduring Biometrics Portable Capability
- Develop/Field IM/IT Infrastructure
- Improve Biometrics Enabled Intelligence (BEI)
- Improve Identity Superiority Capability



*Foundation*



*Integration*



*Fusion*

# How do we bridge the gap?



*Foundation*



*Integration*



*Fusion*

# Military Cooperation

- United States
- United Kingdom
- Australia
- NATO
- Other Military or Coalition Partners



*Foundation*



*Integration*



*Fusion*

# Other Government Departments (OGDs)

- Transport Canada (TC)
  - Canadian Air Transport Security Authority (CATSA)
- Canada Border Services Agencies (CBSA) (NEXUS)
- Royal Canadian Mounted Police (RCMP)
- Canadian Security & Intelligence Services (CSIS)
- Foreign Affairs & International Trade (FAIT)

# Industry & Academia

- Coordination of Requirements and Priorities
- Research & Development Engagement



*Foundation*



*Integration*



*Fusion*

# How ? ?

- Attend Conferences & Exhibitions
- Simplify & Harmonize Legal & Policy Regulations
- Define & Implement Standards
- Expand BEI Training & Development
- Share & Implement Lessons Learned
- Implement Biometrics Data Sharing Agreements



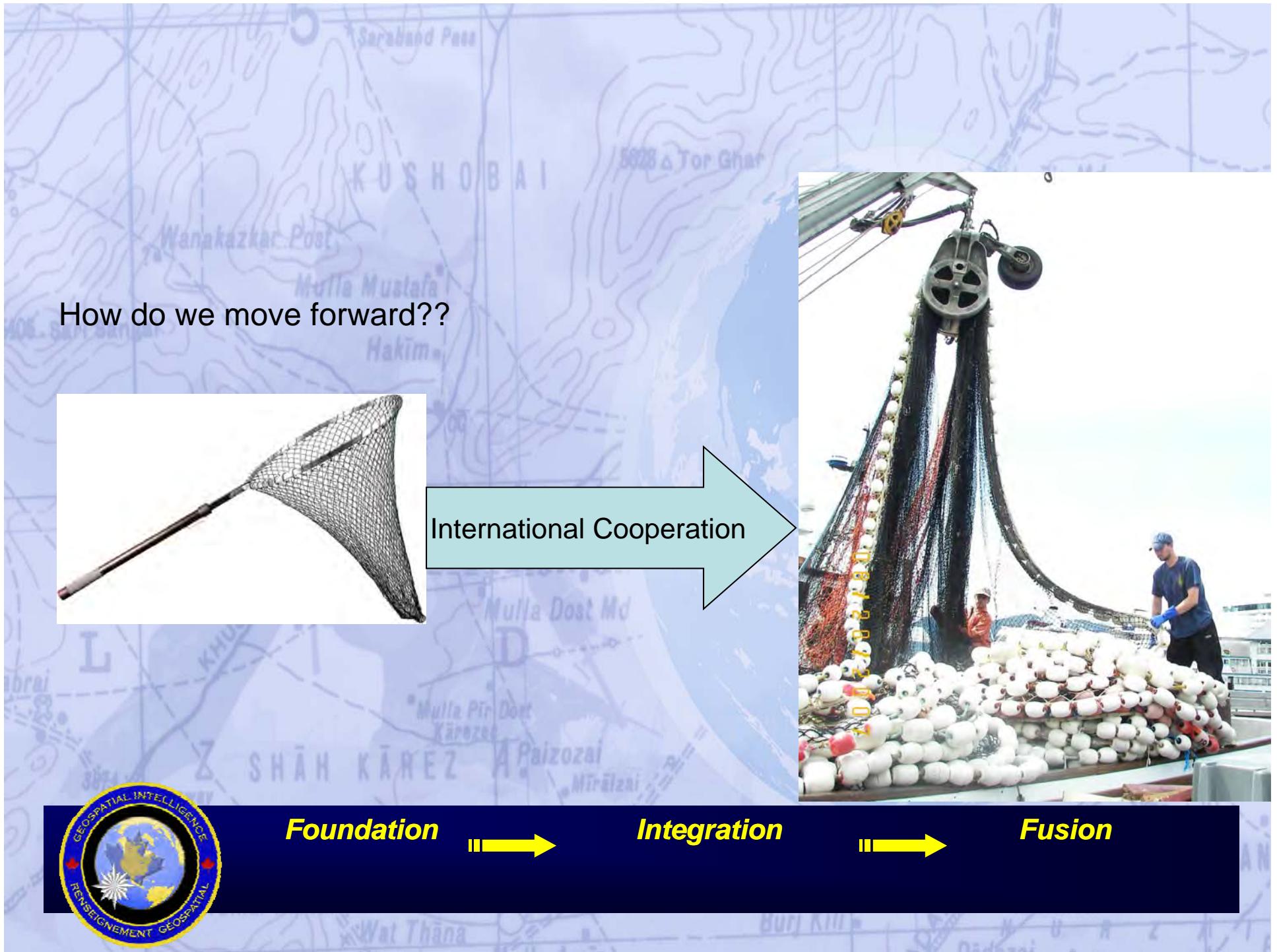
*Foundation*



*Integration*



*Fusion*





# Questions??

Mr. Yves Levesque (D GEO Int)  
[Yves.levesque@forces.gc.ca](mailto:Yves.levesque@forces.gc.ca)  
613-995-4478



*Foundation*



*Integration*



*Fusion*

# Federal Bureau of Investigation Criminal Justice Information Services Division

## Biometrics Screening Programs Panel

January 2010



## CJIS Division Mission

- ▶ The mission of the CJIS Division is to equip our law enforcement, national security, and intelligence community partners with the criminal justice information they need to protect the United States while preserving civil liberties.



# Executing the FBI's mission requires intersecting with government partners and nongovernmental entities



## The FBI deploys biometrics as critical tools for criminal and counterterrorism investigations

Traditional biographic, paper-based identity documents are no longer practical or sufficient



- ▶ Biometrics are the most definitive, real-time identity management tools currently available



## The FBI has operational fingerprint and DNA systems, as well as a multimodal biometric system under development



IAFIS: The nation's fingerprint and criminal history system of more than 64 million subjects provides automated search capabilities 24 hours a day, 365 days a year with criminal responses sent in less than 2 hours and civil responses in less than 24 hours



NGI: Upgrading and expanding the IAFIS system, NGI will collect biometric modalities beyond fingerprints and facilitate increased sharing of biometric data



BCOE: FBI's hub for developing new and advanced biometric capabilities to solve crimes and protect national security. BCOE will centralize and build upon the FBI's biometric systems and expertise

# Next Generation Identification (NGI) Project Background

## Drivers

- Flexibility
- Capacity
- Accuracy
- Response Times
- Availability
- Additional Functionality
- Interoperability

## Objectives

- Faster more efficient identification processing with more accurate results
- More complete Criminal History Record Information database
- Solve more crimes through latent processing
- Provide latent palm print search capabilities

## Capabilities

- Enhanced IAFIS Repository
- Advanced Fingerprint Identification Technology
- Interstate Photo System
- National Palm Print System
- Disposition Reporting Improvements
- Quality Check Automation
- Future Biometrics



**NGI will provide the FBI and its partners state-of-the-art multimodal biometrics identification**



Accuracy



Scalability



Flexibility

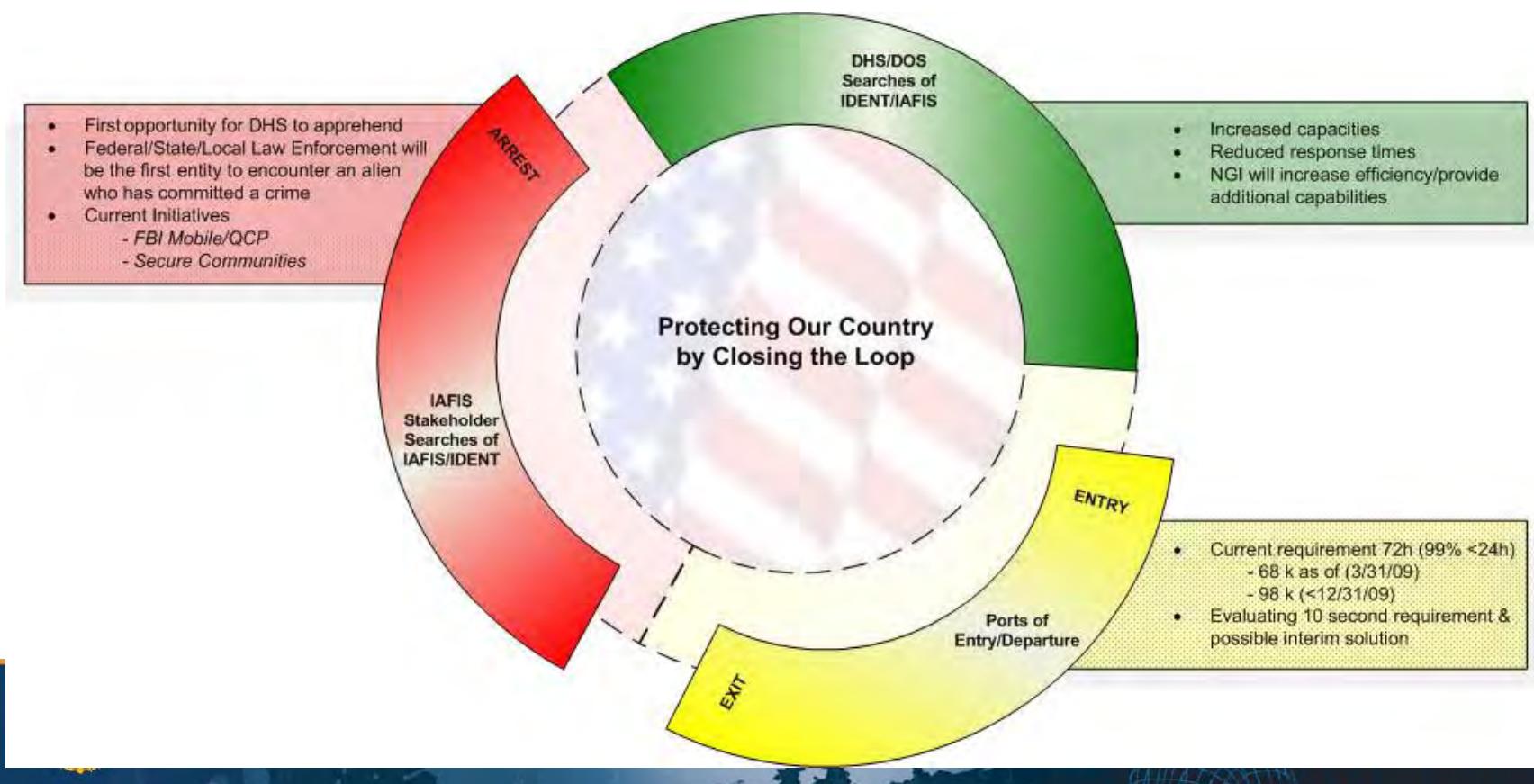


Interoperability



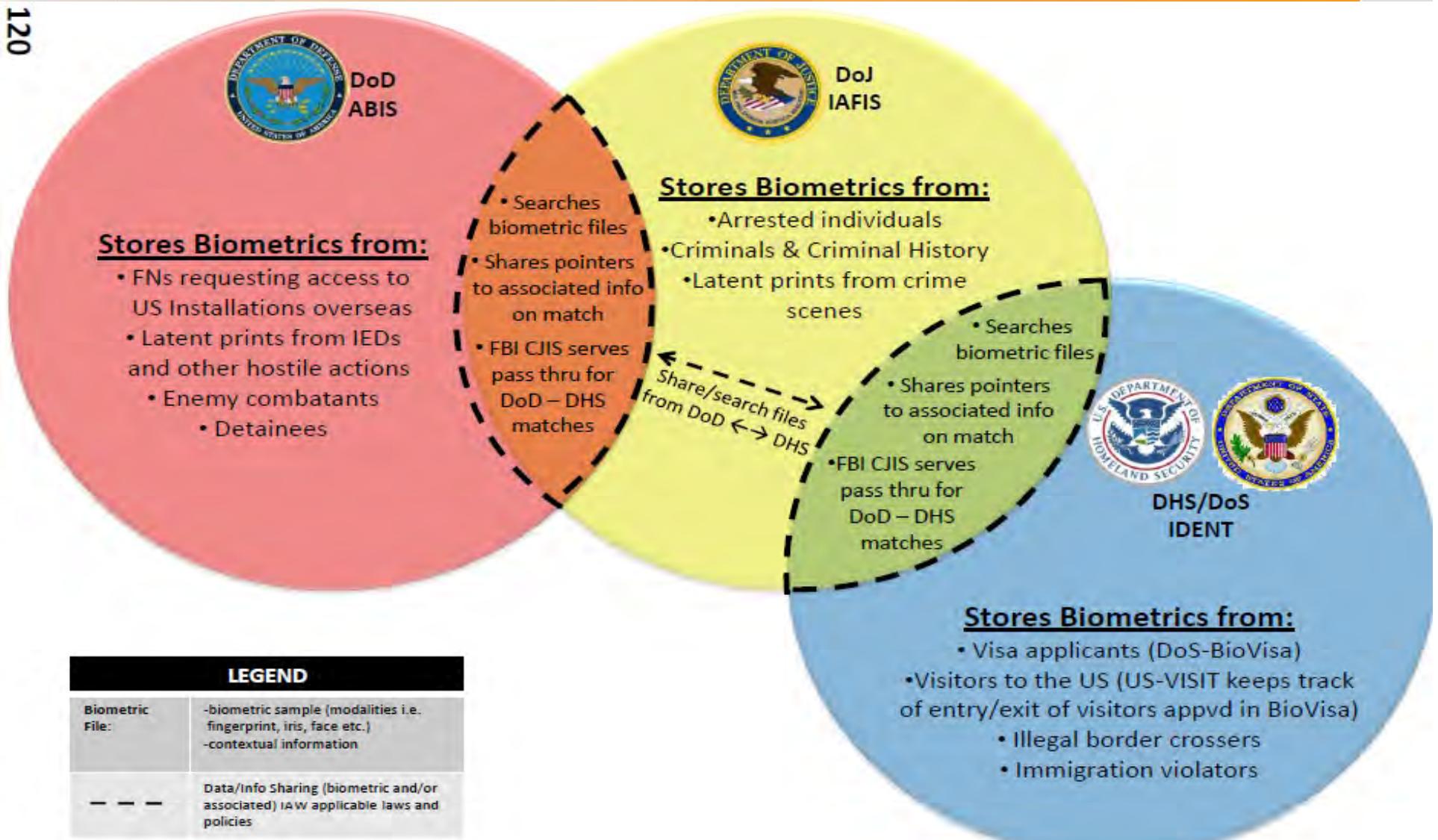
# In 2005, the FBI created the Biometric Interoperability Program to establish interoperability between the FBI's IAFIS and other biometric systems

- ▶ The FBI is currently interoperable with DoD ABIS and DHS IDENT
  - The DoD ABIS system is contained within the CJIS Data Center
  - Criminal history and immigration identity information is becoming accessible and shared among other Federal, State, Local and Tribal law enforcement agencies, as well as authorized non-criminal justice agencies

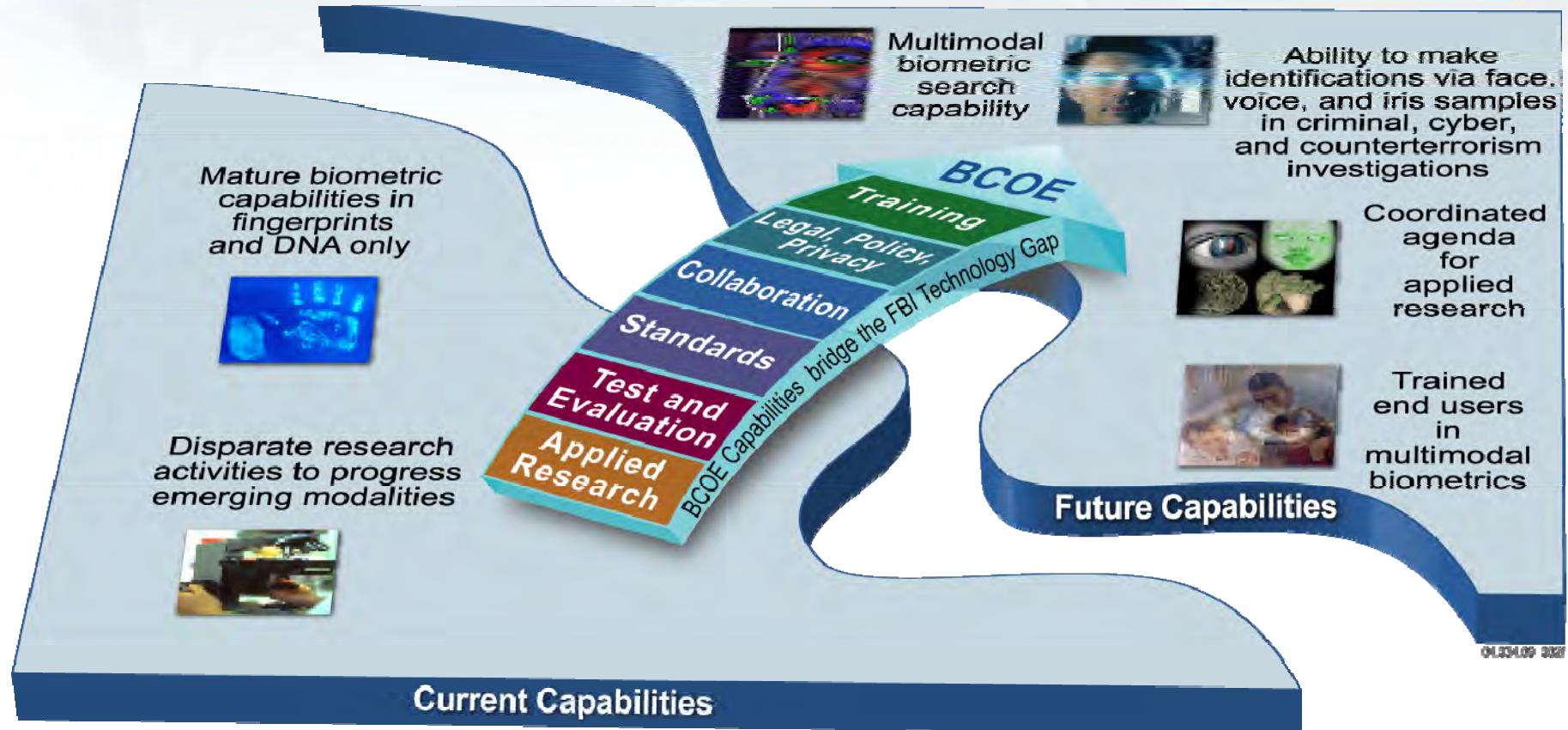


# DoD – DOJ – DHS

120



In 2007, the FBI established the Biometric Center of Excellence to bridge the biometric technology gap



The BCOE is the FBI's focal point to foster collaboration, improve information sharing, and advance the adoption of optimal biometric solutions



# **Biometrics & Privacy**

**Nancy Libin**  
**Chief Privacy and Civil Liberties Officer**  
**Department of Justice**

National Defense Industrial Association  
2010 Biometrics Conference  
January 20, 2010

# Forms of Identification

- Something you have
- Something you know
- **Something you are**

# Uses of Biometrics

- Verification vs. Identification
  - Verification: Am I who I say I am? (1:1)
  - Identification: Who am I? (1:Many)
- Authorization vs. Surveillance
  - Access
  - Monitoring

# Benefits

- May be more secure
- Possible deterrent
- May prevent identity fraud
- Convenient

# Drawbacks

- If lost, lost forever
- False positives/false negatives
- Possible discrimination
- Privacy

# PRIVACY-Basic Questions

- Who owns the data?
- Which technologies pose the greatest privacy risks?
- Are some uses more appropriate than others?
- Can privacy risks be mitigated?

# Informational Privacy

- Data aggregation
- Mission creep
- Redress
- Law enforcement access
- Notice/Transparency
- Accountability

Some applications can enhance privacy....



...while others can erode privacy....



# Issues to Consider

- Consent vs. Non-Consent
- Opt-in vs. Mandatory
- Verification vs. Identification
- Public vs. Private
- Individual vs. Institutional Ownership
- Local vs. Central Storage
- Template vs. Stored Image
- Audit and Oversight
- Backup System

# Privacy Protections

- Limit scope of collection
- Limit duration of retention
- Limit data aggregation
- Encrypt data
- Provide authorization controls
- Provide effective and timely redress
- Disclose purpose of system
- Allow for disenrollment
- Protect confidentiality of decisions

# **DHS Science & Technology:**

# **Biometrics & Identity Management**

**Dr. Sharla Rausch, Director  
Human Factors/Behavioral Sciences Division**

Science and Technology Directorate  
Department of Homeland Security

**January 21, 2009**



**Homeland  
Security**  
Science and Technology

# Human Factors

Behavioral Sciences Division

## Vision:

A safer, more resilient nation that incorporates the human dimension into homeland security analysis, operations and policy development.

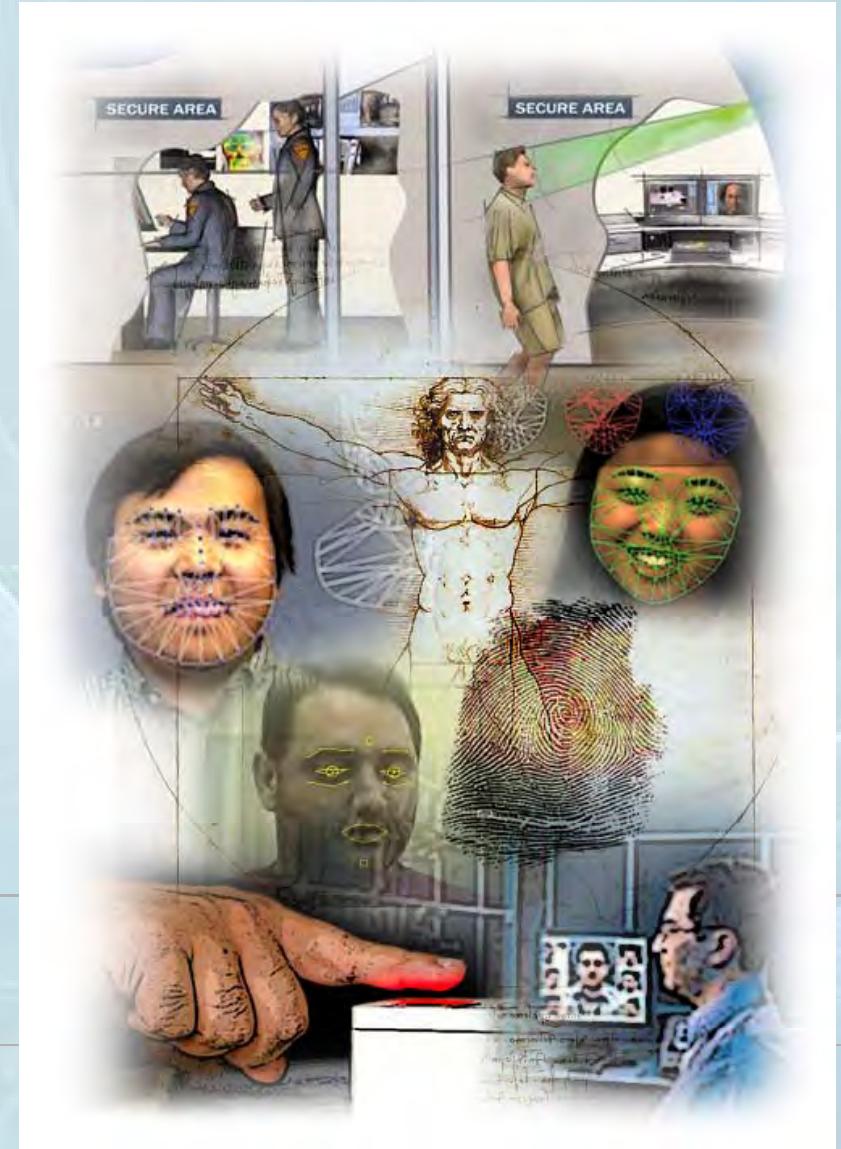
## Mission:

We will advance national security by developing and applying the social, behavioral, and physical sciences to improve identification and analysis of threats, to enhance societal resilience, and to integrate human capabilities into the development of technology.

DHS Customer Components: TSA, US-VISIT, USCIS, ICE, SCO, USSS, FEMA, OI&A, USCG, State & Local, S&T Divisions



**Homeland  
Security**  
Science and Technology

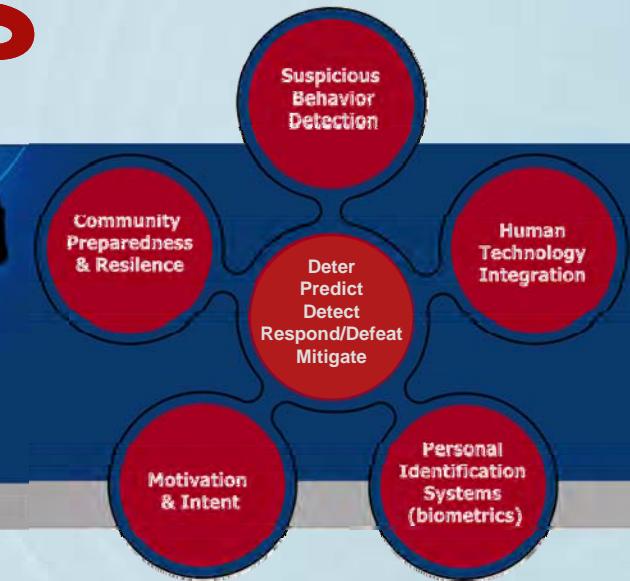


# Human Factors

## Behavioral Sciences Division



Know our enemies, understand ourselves: put the human in the equation



### Motivation & Intent

Enhance the capability of the Department to analyze and counter terrorist motivation, intent, and behavior.

### Suspicious Behavior Detection

Improve screening by providing a science-based capability to identify unknown threats indicated by deceptive and suspicious behavior.

### Personal Identification Systems (Biometrics)

Improve screening by providing a science-based capability to identify known threats through accurate, timely, and easy-to-use biometric identification and credentialing validation tools.

### Community Preparedness & Resilience

Enhance preparedness and mitigate impacts of catastrophic events by delivering capabilities that incorporate social, psychological and economic aspects of community resilience.

### Human Technology Integration

Enhance safety, effectiveness, and usability of technology by systemically incorporating user and public input.



**Homeland  
Security**  
Science and Technology

# Human Factors

Behavioral Sciences Division

## Drivers for the DHS Biometrics S&T Program

*Prevent terrorists from operating effectively against U.S.*

- Know who they are and what they are planning to do
- Impede their ability to recruit, train, obtain finances, acquire weapons (CBRNE), communicate and travel
- Disrupt their activities – surveillance, staging, rehearsal, attack – at all levels of the homeland security enterprise
- Remove dangerous people

*Developing capabilities to consistently and positively identify those seeking entry into the U.S. is vital to this effort*



**Homeland  
Security**  
Science and Technology

# Human Factors

Behavioral Sciences Division

## Drivers for the DHS Biometrics S&T Program

*Prevent illegal entry of people, weapons or contraband into U.S.*

- Deter those who would enter the country illegally or import contraband
- Encourage legal immigration and lawful, secure commerce
- Impede ability to cross border except at designated ports of entry
- Prevent admission of dangerous people while facilitating legitimate travel

*Developing capabilities to consistently and positively identify those seeking entry into the U.S. is vital to this effort*



**Homeland  
Security**  
Science and Technology

# Human Factors

Behavioral Sciences Division

## Drivers for the DHS Biometrics S&T Program

*Protect continuity of systems fundamental to societal stability and security*

- Impede the ability to disrupt or weaponize critical infrastructure
- Implement a cascading Federal/State/community/individual system of resilience through preparedness and integrated emergency management
- Ensure resiliency of functions critical to public health and safety, government and essential services



*Developing capabilities to consistently and positively identify those seeking entry into the U.S. is vital to this effort*

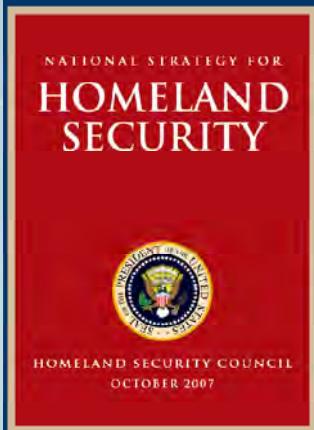


**Homeland  
Security**  
Science and Technology

# Human Factors

## Behavioral Sciences Division

## Drivers for the DHS Biometrics S&T Program

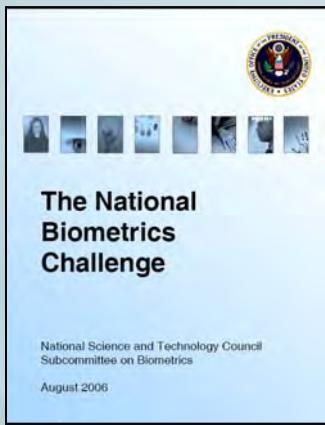


***“In the face of resourceful terrorists, however, we must continue to expand the US-VISIT program’s biometric enrollment from two fingerprints to ten fingerprints, as well as leverage science and technology to enable more advanced multi-modal biometric recognition capabilities in the future that use fingerprint, face, or iris data.”***

### **- National Strategy for Homeland Security, Homeland Security Council, October 2007**

*“...agencies are to place emphasis on the priorities outlined in The National Biometrics Challenge and the resulting agenda developed by the NSTC Subcommittee on Biometrics and Identity Management.”*

## **- OMB and OSTP FY2009 R&D Budget Priorities ([www.ostp.gov](http://www.ostp.gov))**



DHS People Screening IPT

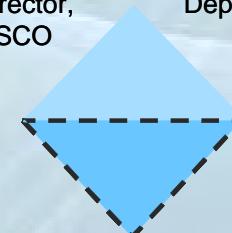
**Kathy Kraninger**  
Director,  
SCO

## **Michael Ayles** Deputy Director, **CIS**

**Sharla Rausch**  
Director,  
Human Factors

## Acquisition

**Bob Mocny**  
Director, US-VISIT



# Human Factors

Behavioral Sciences Division

## Biometrics: *DHS's Unique Challenges*

- DHS has some unique Biometric challenges for screening operations
  - Scale and diversity of screening sites
  - Accommodation of existing DHS practices
    - Workload, wait times and throughput
  - Harsh lighting and environmental factors
  - Extreme Outdoor Mobile Conditions
  - Non-cooperative users
  - Field-collected samples of mixed quality
  - Real-time access to match results across the DHS enterprise and interoperability with mission partners
- These challenges must be addressed for widespread deployment of biometrics



San Ysidro Border Crossing



Poker Creek Border Crossing



**Homeland  
Security**  
Science and Technology

# Human Factors

Behavioral Sciences Division

## Compelling Need for Biometrics

### US-VISIT Program:

- More than 100 Million immigrant visit records
- Protecting 300 U.S. ports of entry
- 500 Million border crossings each year
- 9 Million visa applications and 50,000 asylum requests each year
- 30,000 immigration benefits applications processed each day

### Statutory and Regulatory Biometric Mandates:

- Freezing identity & searching watch lists
- Conducting criminal background checks & reducing fraud
- Improving border and transportation security
- Granting benefits and credentials

### Support to other Federal, State and First Responders



A U.S. Customs and Border Protection officer demonstrates how an international visitor should place her fingers on the scanner during the entry process.



**Homeland  
Security**  
Science and Technology

# Human Factors

Behavioral Sciences Division

## **The *Hard Sciences* in Biometrics & Identity Management**

Chemistry/Biology:

Low Cost and Rapid DNA

Mathematics:

Multi-Biometric Fusion

Performance Modeling

Physics:

Mobile 10-print Slap Capture

Robust Face/Iris Capture

Contactless Fingerprints



**Homeland  
Security**  
Science and Technology

# Human Factors

Behavioral Sciences Division

**The *Hard Sciences* in Biometrics & Identity Management**



**Homeland  
Security**  
Science and Technology

# Human Factors

Behavioral Sciences Division

## **The *Harder* Sciences in Biometrics & Identity Management**

### Usability:

Biometric Quality Assessment

### Standards:

InterNational Committee for IT Standards (INCITS) M1 Tech. Comm.

International Organization for Standards (ISO) JTC 1/SC 37

### Acceptability:

Community Perceptions of Technology Panel

M1.6 and SC37/WG-6: Cross Jurisdictional and Societal Issues

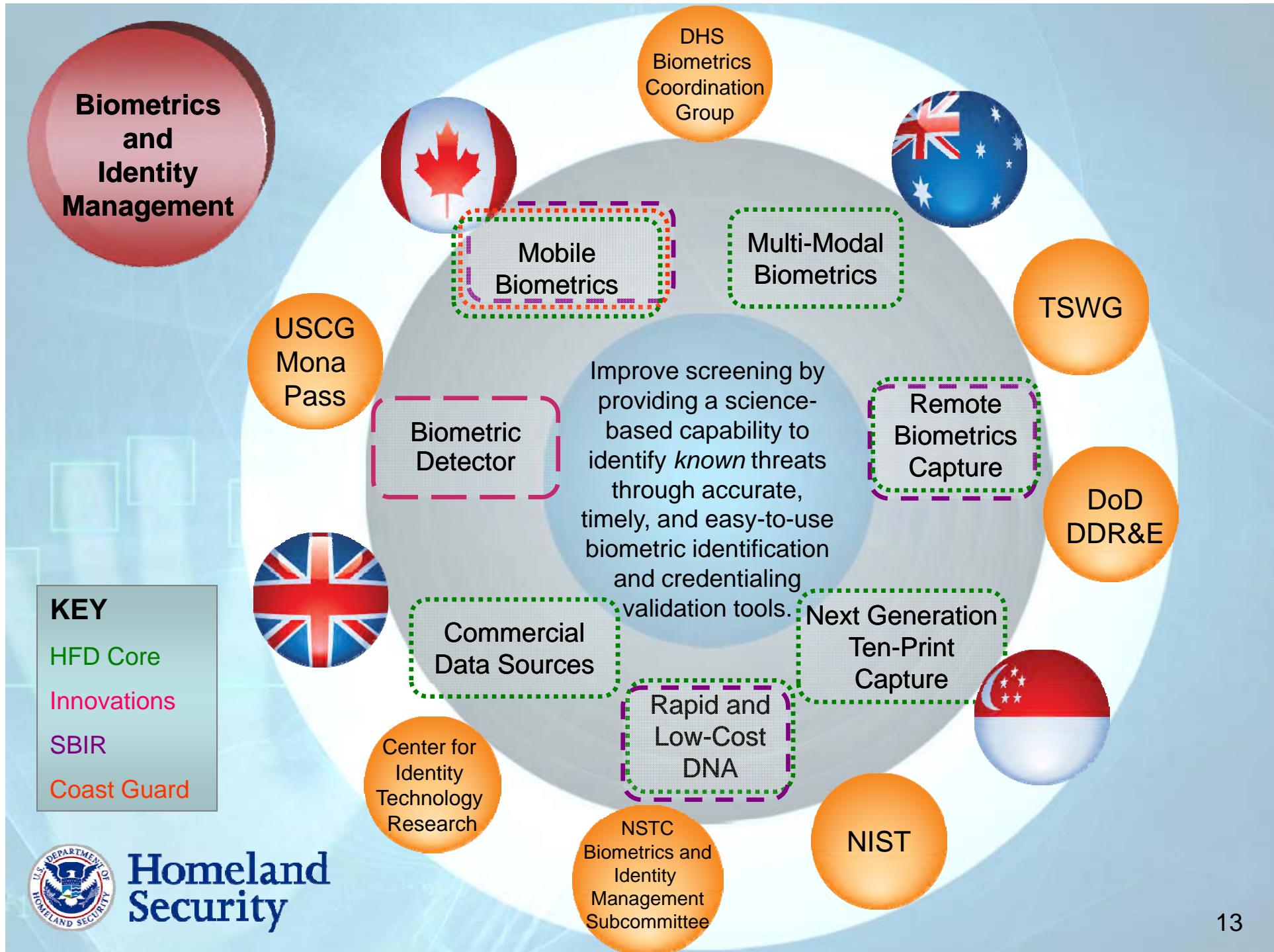
### Test and Evaluation:

Multi-Biometric Grand Challenge (MBGC) and Experiment (MBE)

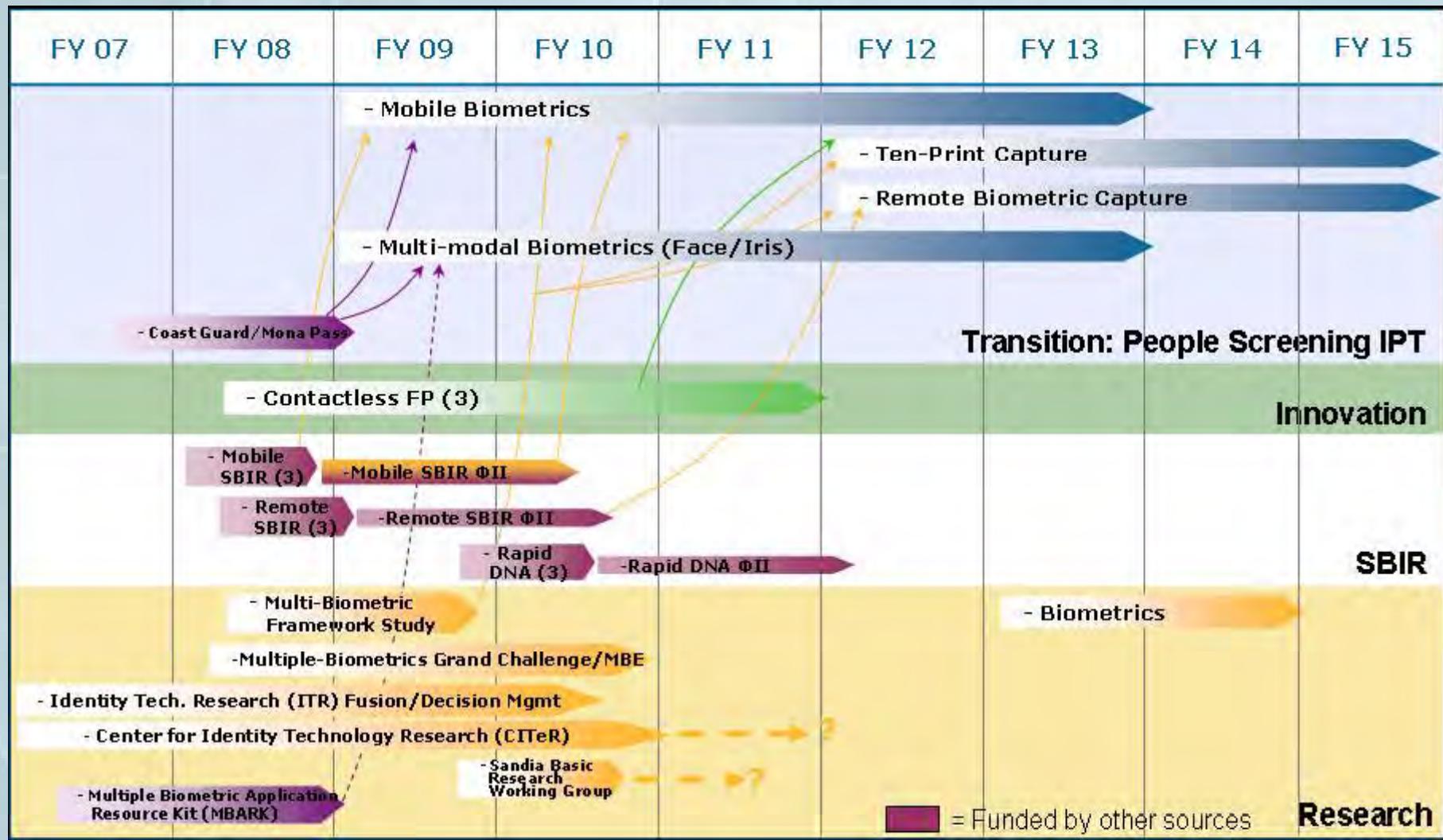
National Voluntary Laboratory Accreditation Program (NVLAP)



**Homeland  
Security**  
Science and Technology



# DHS S&T Biometrics Program Timeline



# Human Factors

Behavioral Sciences Division

## Indispensable Resources

[www.Biometrics.gov](http://www.Biometrics.gov)

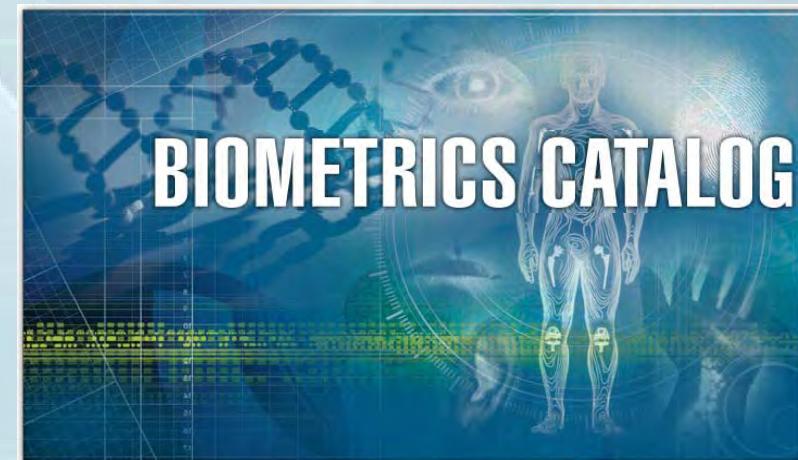
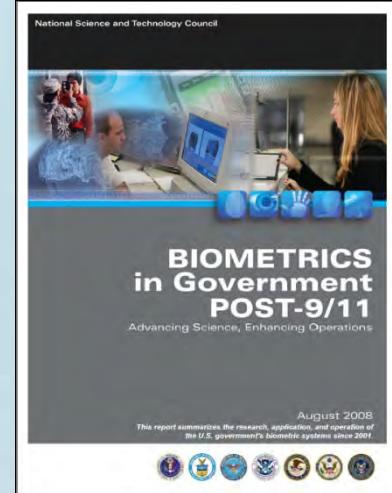
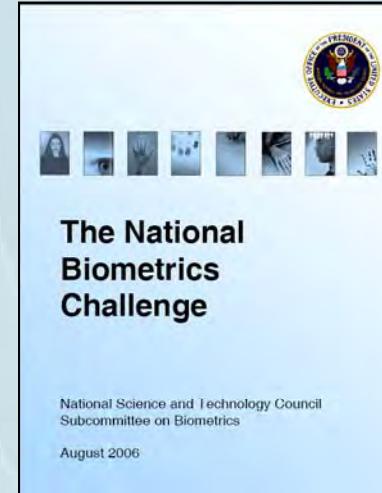
Central source on Federal government biometrics-related activities

[www.BiometricsCatalog.org](http://www.BiometricsCatalog.org)

U.S. Government-sponsored database of public information about biometric technologies kept current by its users, who add information as it becomes available – Free to use and update

[www.Biometrics.org](http://www.Biometrics.org)

Biometrics Consortium web site with free discussion bulletin board and annual conference news



**Homeland  
Security**  
Science and Technology

**Biometrics.gov**



# Homeland Security

---

## Science and Technology

---



**Homeland  
Security**  
Science and Technology

# Backup Slides



**Homeland  
Security**  
Science and Technology

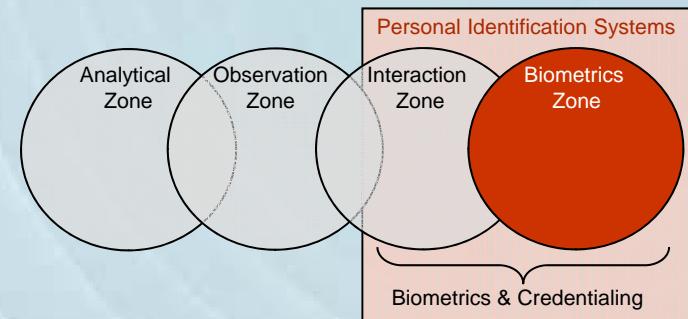
# Human Factors

Behavioral Sciences Division

## Multi-modal Biometrics: *Using the Full Range of Identification Tools*

### Goal:

- Develop Multi-modal biometric tools (fingerprint, face, and iris) to accurately and rapidly identify known terrorists
- Develop a framework to facilitate the integration of biometric technologies across the DHS operational mission space.



### Approach:

- Support development of interoperable biometrics tools and technologies
- Develop multi-modal biometrics collection capability suitable for use in DHS operational environments
- Develop fusion technologies to synthesize identity matches from DHS field-collected (non-ideal quality) multi-biometric data

### Payoff:

- Improved biometrics-based identification of known terrorists
- Increase throughput of lawful travel across U.S. borders



# Human Factors

Behavioral Sciences Division

## Mobile Biometrics: *Biometrics on the Front Lines*

### Goal:

- Spiral development of mobile multi-modal biometric sensors and technologies to provide accurate identification capabilities anywhere in the DHS area of responsibility

### Approach:

- Collaborate with DHS components to identify and document requirements for mobile biometrics new and existing DHS operations
- Develop technologies, sensors, and components for integration in future multi-modal mobile biometrics collection systems
- Leverages activities of DHS S&T, USCG (Mona Pass), CBP, CIS, ICE, TSA, and USVISIT

### Payoff:

- Biometric screening can occur at non-fixed sites beyond U.S. borders, between ports of entry, and within secure sites/facilities



**Homeland  
Security**  
Science and Technology

# Human Factors

Behavioral Sciences Division

## Mobile Biometrics – Accomplishments

### *Handheld Biometric System Pilot in the Mona Pass*

Goal:

- Real-world operational pilot of Coast Guard maritime mobile biometrics technologies in the Mona Pass.
- The pilot identified strengths and shortfalls associated with the use of mobile biometrics.

S&T and Homeland Security Payoff:

- Timely identification of interdicted immigrants to determine if they are on a watch or wanted list. 90% of all yolos have at least one hit against IDENT.
- 100% conviction rate since the implementation of biometrics.
- Results of pilot informs S&T's FY09 Mobile Biometric transition project of specific real-world operational shortfalls that exist with the use of mobile biometrics devices.



**Homeland  
Security**  
Science and Technology

# Human Factors

Behavioral Sciences Division

## Mobile Biometrics – Accomplishments

### *Handheld Biometric System Pilot in the Mona Pass*

Metric	Number Encountered	% of total possible
Biometrics Collected	2598	99% of persons encountered
Database Matches	639	25% of records collected
Prosecutions	330	52% of matches

~ Data as of September 2009



**Homeland  
Security**  
Science and Technology

# Human Factors

Behavioral Sciences Division

## DHS S&T Innovations Project: Biometric Detector *Touchless Fingerprints*

Goal:

- Develop technologies for efficient, high quality, contactless acquisition of fingerprint biometric signatures

Payoff:

- Ergonomic and user-friendly design provides significantly improved throughput and signal quality
- A fingerprint acquisition device that can be transitioned for implementation across DHS operational mission space
- Customers - US-VISIT, USCIS, CBP, ICE, TSA



**Homeland  
Security**  
Science and Technology

# Human Factors

Behavioral Sciences Division

## Small Business Innovation Research Projects

### Remote Biometrics:

- Three Phase I and one Phase II effort to assess the maximum standoff ranges for capture of multiple biometrics while accurately identifying an individual

### Mobile Biometrics:

- Three Phase I and two Phase II efforts to analyze DHS needs; conduct a technology risk assessment; and develop a prototype mobile multi-biometric device and communications gateway

### Rapid DNA-based Biometrics:

- Three Phase I efforts to analyze DHS needs; conduct a technology risk assessment; and ultimately demonstrate an automated desktop prototype device that verifies identity or kinship within an hour from DNA (deoxyribonucleic acid) samples



**Homeland  
Security**  
Science and Technology

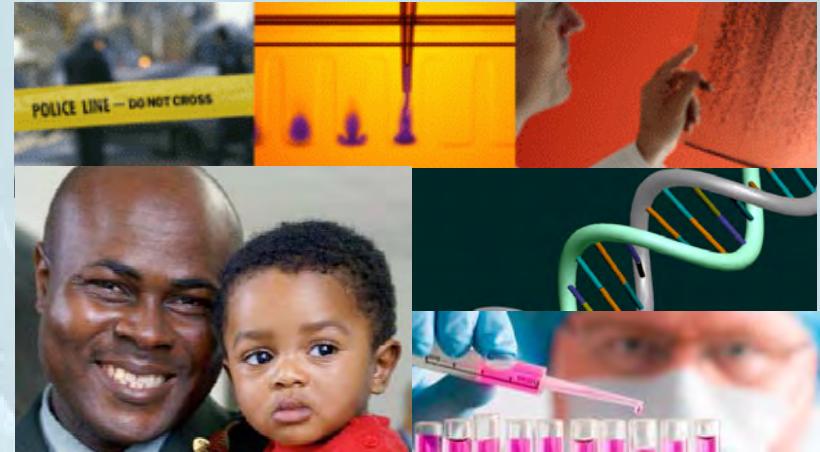
# Human Factors

Behavioral Sciences Division

## Rapid DNA-Based Screening: *Reducing Immigration Fraud*

### Goal:

- Develop rapid DNA-based screening technology to verify family relationships (kinship) and identity of those seeking asylum or immigration into the United States; children put up for overseas adoptions; and mass-casualty identifications



### Approach:

- Definition of DHS metrics and evaluation of potential small business approaches through the DHS SBIR program
- R&D to automate and integrate DNA processing steps
- Collaborative program with DoD, TSWG and DOJ to create a desktop prototype system in 18 months

### Payoff:

- DNA screening for kinship is reduced from weeks to under an hour, from \$500 to \$100 per sample, and conducted in-house vs. external labs



**Homeland  
Security**  
Science and Technology

# Human Factors

Behavioral Sciences Division

## Technology Acceptance and Integration Program: *Incorporating Community Perspectives into Technology Development*

### Goal:

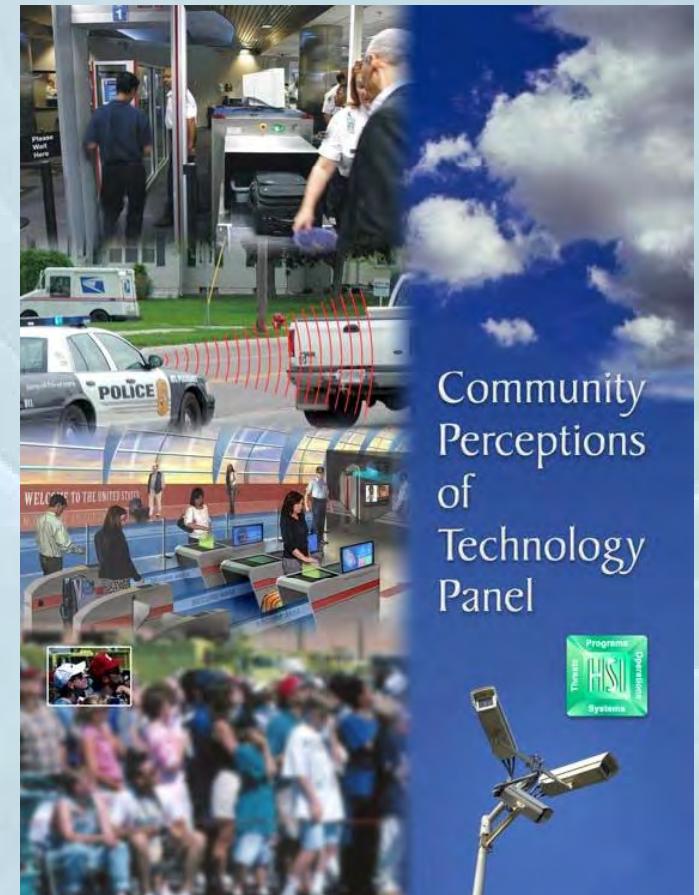
- To successfully develop and adopt application specific, publicly acceptable technologies and processes.

### Approach:

- Community Perceptions of Technology (CPT) Panel focuses on a selected technology/process.
- Experts selected from industry, public interest, and community-oriented organizations to participate.
- Qualitative data collected is used to inform operational processes, to develop and deploy technology, and to guide the design of additional research tools.



**Homeland  
Security**  
Science and Technology



Community  
Perceptions  
of  
Technology  
Panel

# Human Factors

Behavioral Sciences Division

## *Incorporating Community Perspectives into Technology Development*

### CPT Panels 2008:

- February 2008: Microwave Vehicle Stopping
- May 2008: Raman Spectroscopy- IED Standoff Explosive Detection
- August 2008: Mobile Biometric Technology
- December 2008: Nonlinear Acoustic IED Standoff Threat Detection

### CPT Panels 2009:

- March 1-3: Northern Border Technology- Radio-Frequency Identification (RFID) Registration and Low Resolution Imaging Technology
  - Joint panel with the Canadian Government
- August 5: Imaging Technology
- TBD: Biometrics
  - Joint panel with the UK



**Homeland  
Security**  
Science and Technology



# Homeland Security

---

## Science and Technology

---



**Homeland  
Security**  
Science and Technology



# Personal National Identification System National Population Registry Mexico

January 21st, 2010

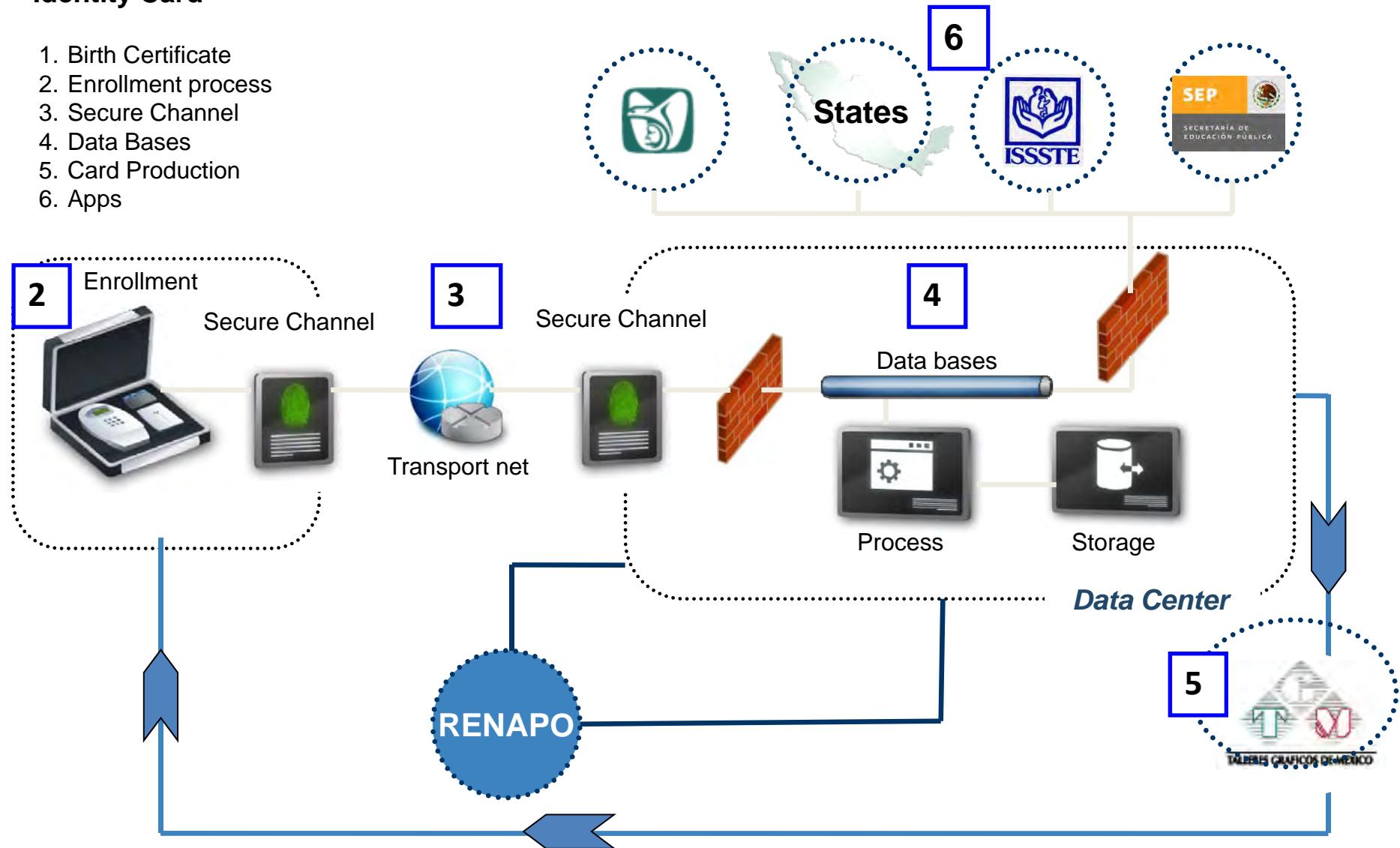


Documento de trabajo reservado en términos del Art. 14 de Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental

# Operational Diagram

## Identity Card

1. Birth Certificate
2. Enrollment process
3. Secure Channel
4. Data Bases
5. Card Production
6. Apps



Documento de trabajo reservado en términos del Art. 14 de Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental

People attend the enrollment office (or mobile unit), where the identity of the person is confirmed by webservices accesing the databases of:

- CURP (Code to the Population Registry) (RENAPO validates the identity of people by the use of webservices, achieving over 1 million consults a day)
- Birth Certificate (Today RENAPO has over 96 million birth certificates on database)

**The information considered for the enrollment process is:**

- Facial picture (2D)
- 10 fingerprints
- 2 iris
- Digitalized signature
- Scanning of CURP or birth certificate



The recognition rate for each biometry is\*:

- Facial picture: 71.5%;
- 10 fingerprints; 95%; and
- 2 iris; 97.4%.

*\*Data calculated with a basis of 0.01% FAR (False acceptance rate)*

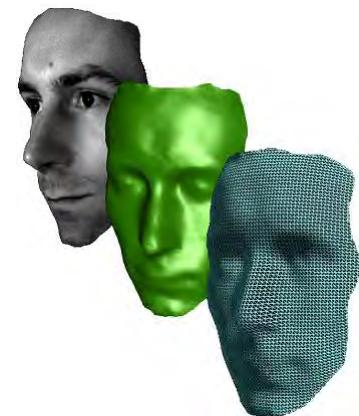
On November 23rd, RENAPO published the manuals for registration of people, which are based on the standard published by the National Institute of Standards and Technology (ANSI NIST ITL 2008).

In recent years, face recognition systems, have improved their accuracy mostly because of the power of search engines, the 3D modeling applications, and the devices used for enrollment.

Eventhough, enrollment process for a population over 100 million people is a challenge for many reasons:

- Non – controlled conditions for enrollment process (illumination for instance), which directly impacts the quality of the file (this will happen when using mobile enrollment units)
- Time used for the enrollment (for 3D applications, certain conditions have to be met, which takes more time enrolling people)

Despite these conditions, face recognition systems is one of the most accepted technologies, due to its link to ID cards and the need of a picture in almost every biometric recognition system.



Lately, many countries have realised the importance of meeting better standards, and getting as much information as they can in order to improve the accuracy of the recognition systems. For example, US Visit program, has almost completed migration from 2 to 10 fingerprints in order to have more control over the visitors to American soil.

The use of 4-4-2 devices help to control the enrollment process, and dramatically decreases the chance of a person faking an identity (fingers can be replaced when enrolling 2 fingerprints).

Fingerprint recognition systems have some disadvantages in open population:

- Construction and farm workers may not be correctly recognised because of the usage of the fingerprint
- Children under 10 years old may not be correctly recognised



Iris recognition systems are one of the technologies with more expectancy of development, because of its accuracy, and the difficulty to fake an iris scan (iris is protected by a transparent membrane, inside of the eye).

Despite the cost of iris scan devices, it would be more expensive to re-enroll people, mostly for a fundamental population registry such as RENAPO.

Other advantage of iris recognition systems is the fact that it is not an intrusive identification method, fact reported in the Privacy Impact Assessment to RENAPO (December 2009).



The National Population Registry is integrated by:

- National Citizen Registry (18+ years old)
- National Youth Registry (under 18 years old)
- Foreigners Catalog (living in Mexican soil)

- Information for both Citizen and Youth Registry is integrated and used by all units in public administration
- Foreigners Catalog information is integrated by the National Migration Institute.

- Personal Information from birth certificate (migratory form for foreigners )
- Biometric Information (face, fingerprints, iris)
- Parents data in the case of children

- Over 2000 enrollment stations will be set by July 2010

- ID Card (Mexicans only)
- Acces to government services
- Acces to private services (such as banking system)

- ID card will have fingerprint minutia encoded in a 2D barcode for offline identification.
- Webservices will be available for online identification (Code of Population + fingerprint)

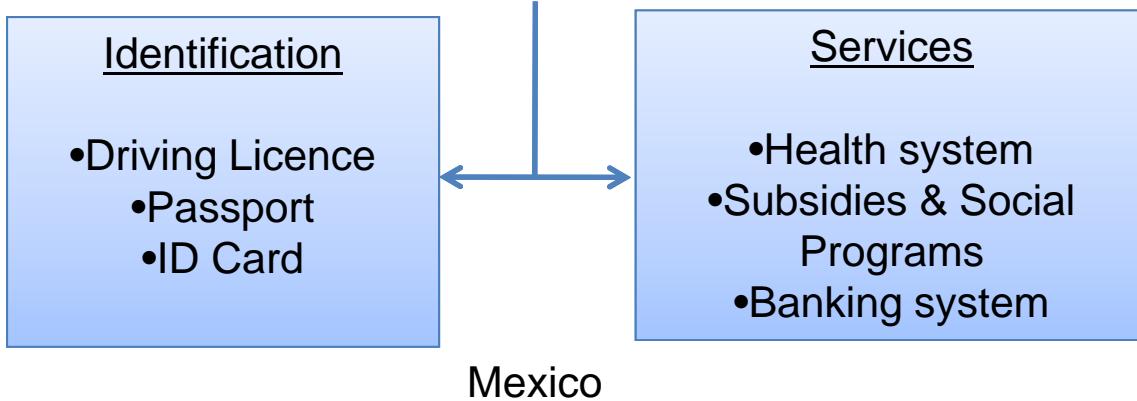


## Mexican ID Card (Sample)



Target

Over 70 million Citizens  
Over 35 million youth



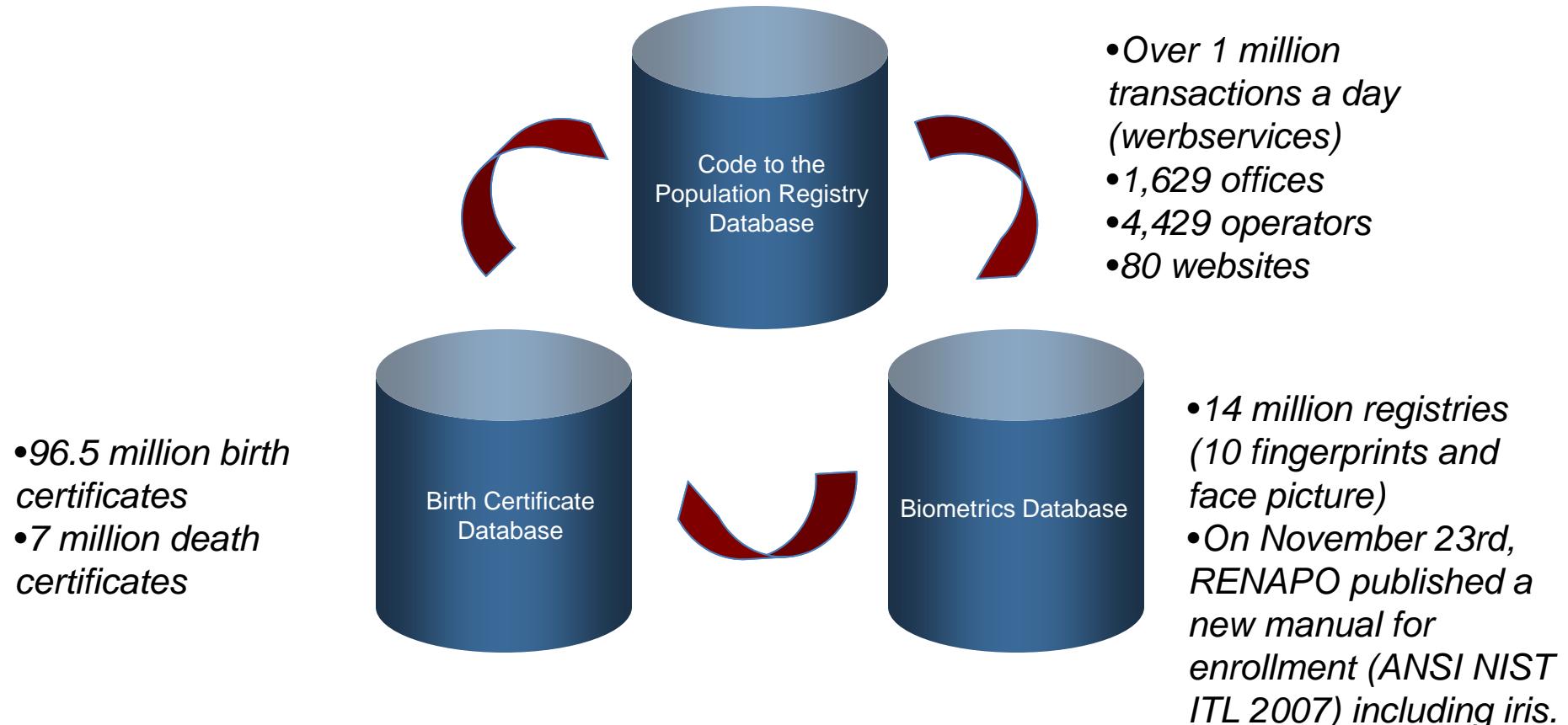
Over 20  
million  
mexicans

Outside  
Mexico

• Webservices will be set in Embassy and Consulates, in order to validate the identity of a person to get an ID card outside of Mexico

Federal and  
local  
government

Embassy  
Consulate



***Southern Border: The objective is to strengthen migration management policy to better regulate the border immigration flows***

***Description:***

- Issue a new *Border Worker Card (BWC)* to allow individuals from *Guatemala and Belize* to work as *temporary workers in the states of Campeche, Chiapas, Quintana Roo and Tabasco*
- Increase the security components of the *Local Visitor Card (LVC)* and *BWC* to meet international standards by including biometrics



- Technology is a tool to implement public policies, which means that we have the responsibility to choose between technologies in order to implement those policies. Technology by itself is not the answer to government obligations.
- Protection of personal data and Privacy Impact Assessments, are practices to be considered in order to have the trust of the population in registry projects. Furthermore, each country has its own policy to personal data protection which has to be complied. (Not every government agency has the attributes to have this information).
- The use of 3 biometrics is set to guarantee that every person has only one single record on the database; to identify a person a single biometric and the Code to Population Registry (CURP) can certify the identity (one to one match). This identification can be done by webservices (online), or by the usage of an ID card.



# National Defense Industrial Association Biometrics Conference Technology and Standards Panel 21 January 2010

DoD Forensic Science & Technology

Jeff Salyards

Program Manager, Science and Technology

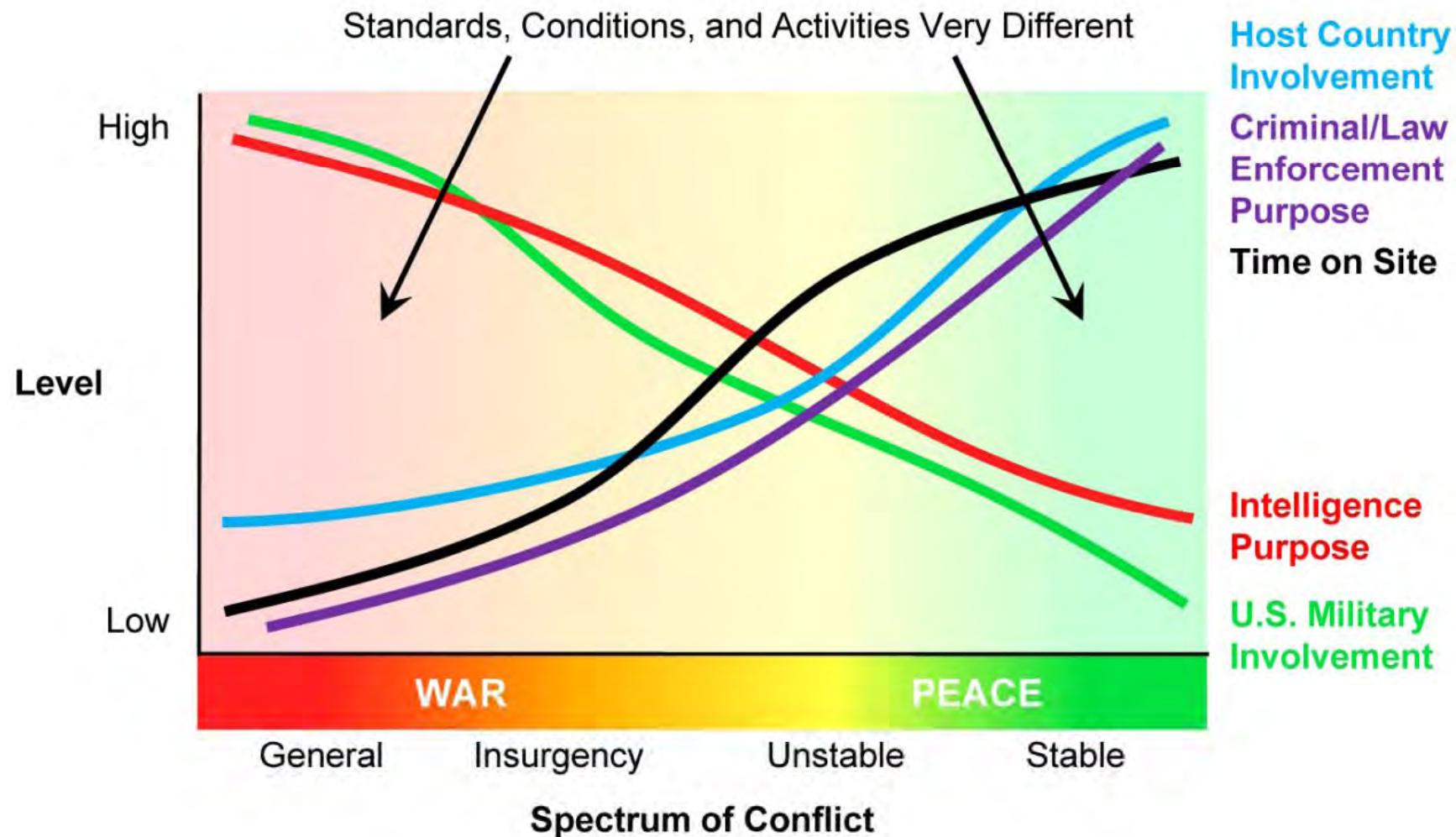
U.S. Army Criminal Investigation Laboratory

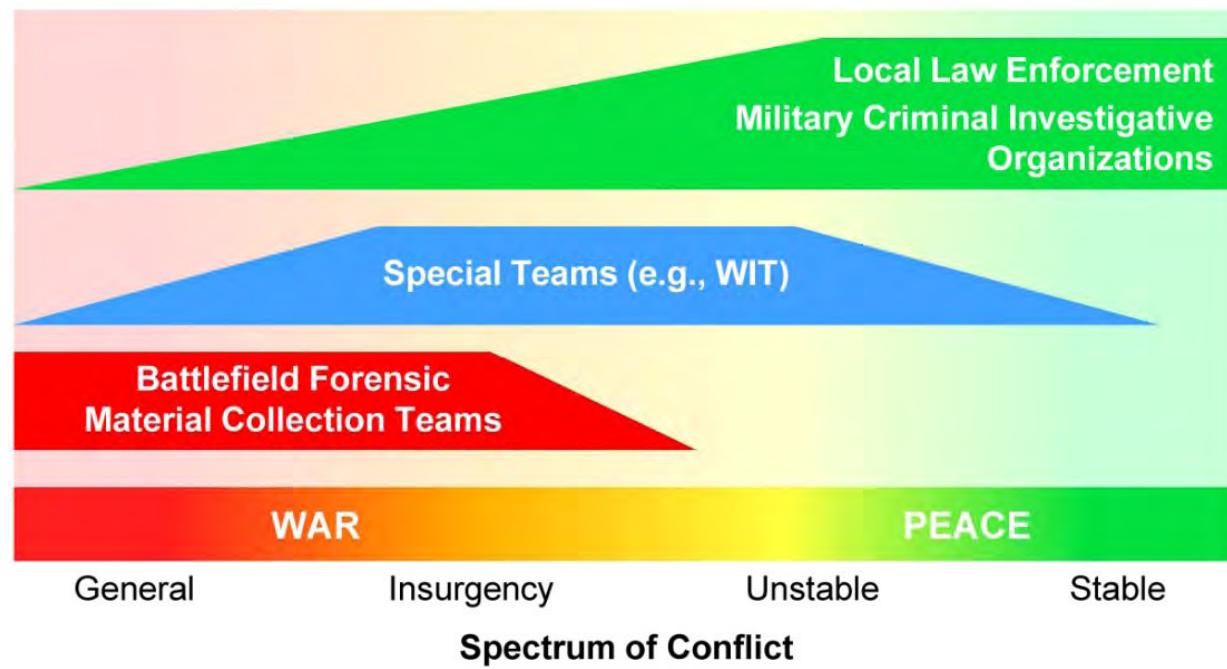
(404) 469-5569 (office)

[jeff.salyards@us.army.mil](mailto:jeff.salyards@us.army.mil)



The opinions or assertions contained herein are the private views of the author and are not to be construed as official or as reflecting the views of the Department of the Army or the Department of Defense.

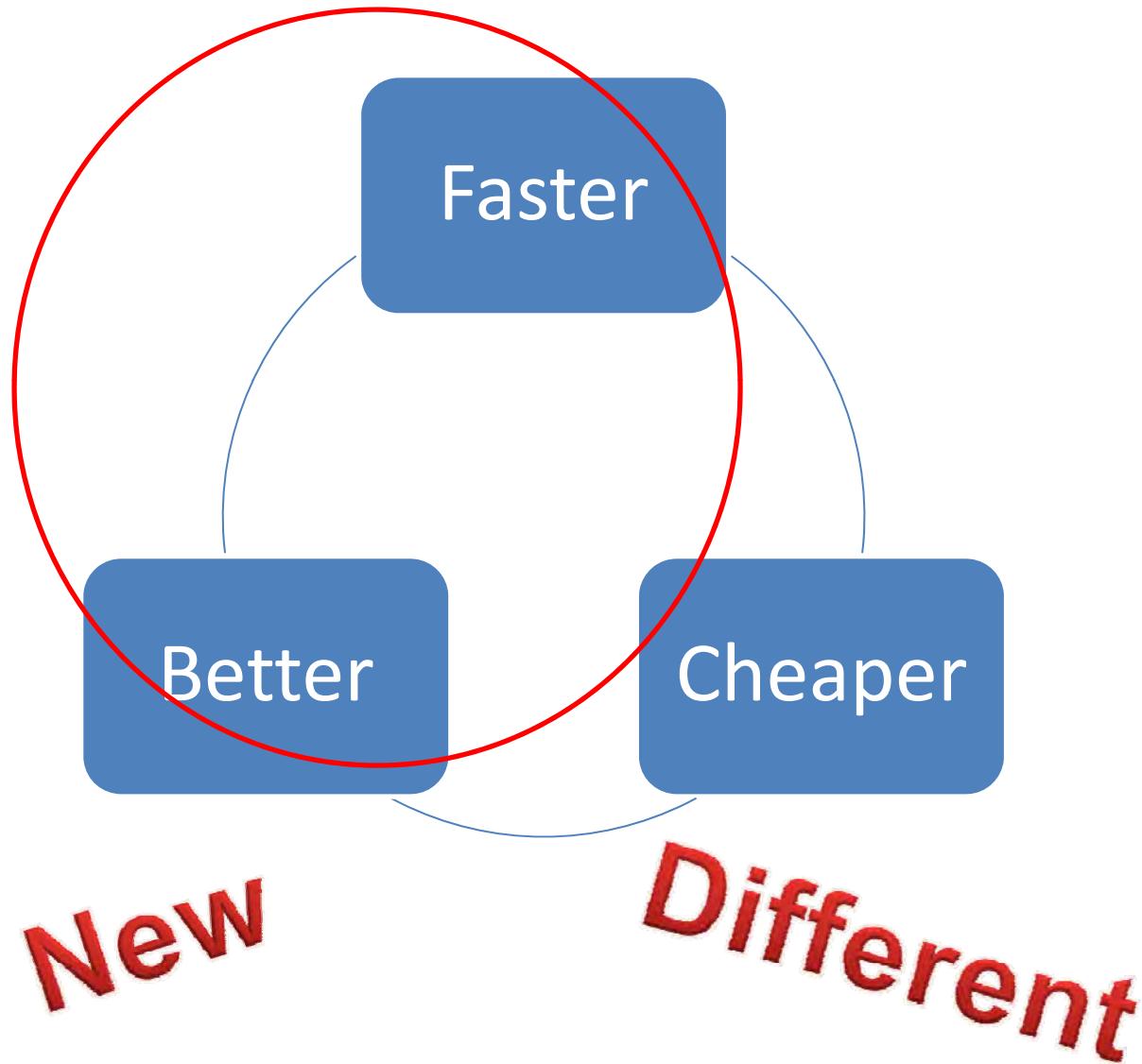






# Roadmap

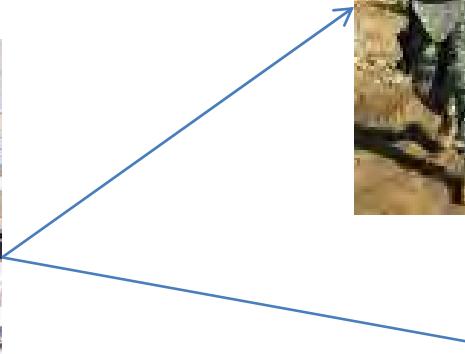
- Centralized vs Decentralized
  - Faster, Better, Cheaper
  - NAS Report
  - Managing Results
- Gaps
  - Existing DoD Projects
  - Future Projects





# Better, Faster, Cheaper

## Smaller, Rugged









# NAS Report

## **STRENGTHENING FORENSIC SCIENCE IN THE UNITED STATES** **A PATH FORWARD**

Committee on Identifying the Needs of the Forensic Science Community

Committee on Science, Technology, and Law Policy and Global Affairs

Committee on Applied and Theoretical Statistics

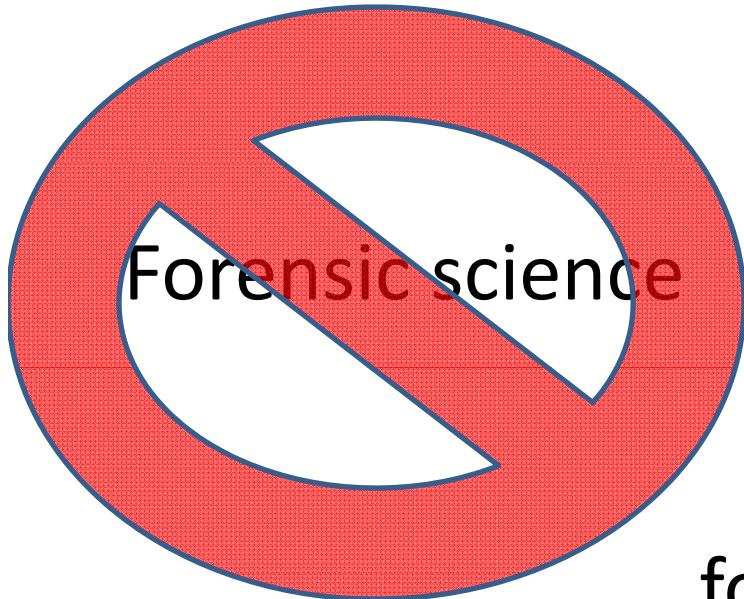
Division on Engineering and Physical Sciences

**NATIONAL RESEARCH COUNCIL OF THE NATIONAL ACADEMIES**  
**THE NATIONAL ACADEMIES PRESS**

Washington, D.C.



# NAS Report – Executive Summary



forensic **S**cience

forensic **\$**cience



# NAS Report – S&T Summary

- Recommendation 3 – NAS Report
  - Establish validity of forensic methods
  - Determine estimates of uncertainty
  - Develop measures of reliability and accuracy
- Recommendation 5 – NAS Report
  - Investigate human observer bias
  - Identify sources of human error
  - Develop model protocols to minimize these errors
- Recommendation 10 – NAS Report
  - Support graduate education programs/fellowships
  - Emphasize multidisciplinary fields
  - Support continuing legal education programs



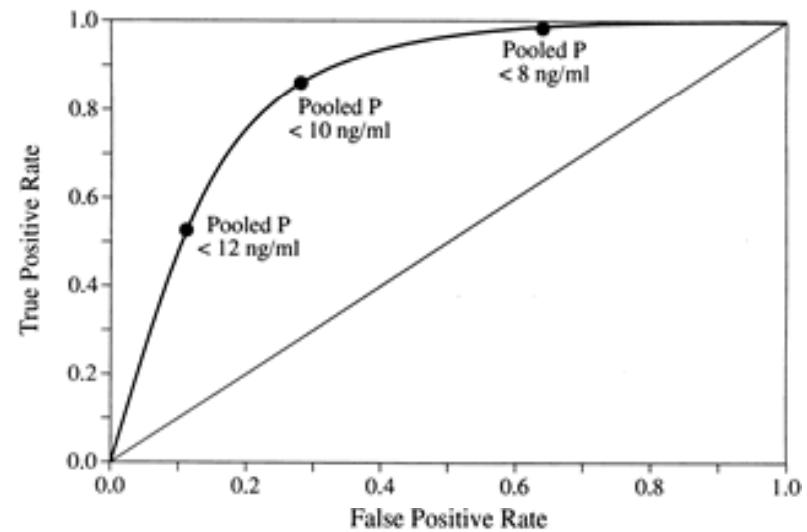
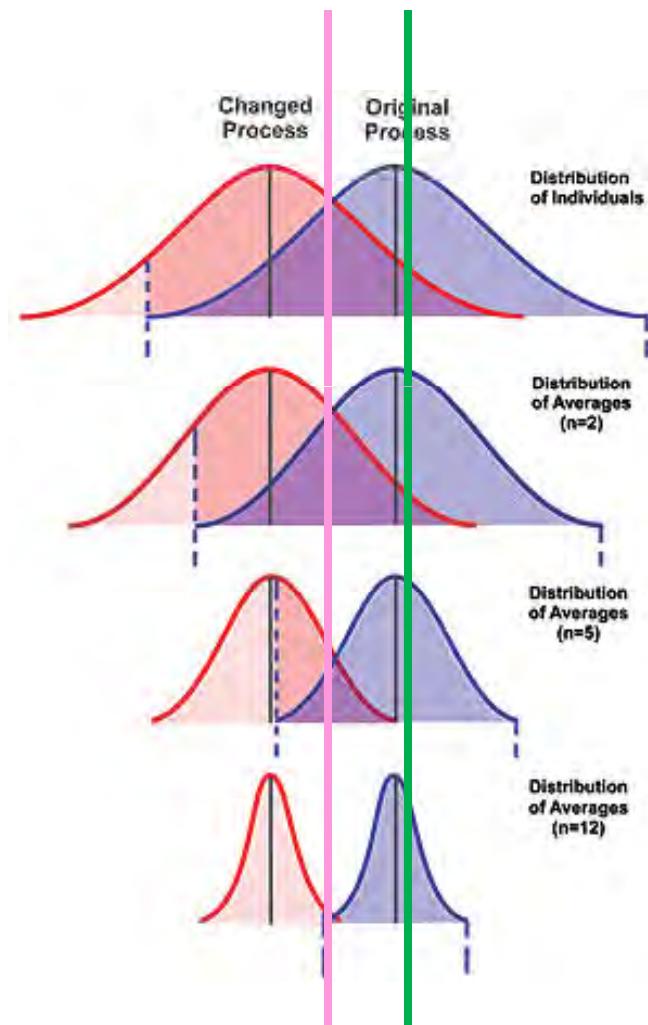
# Recommendation 3 – NAS Report



Peer-reviewed research on uncertainty, accuracy and reliability



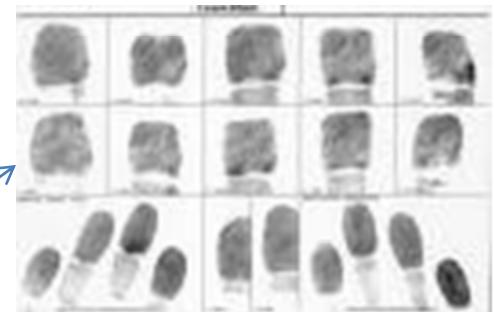
# Recommendation 3 – NAS Report



Peer-reviewed research on uncertainty, accuracy and reliability



# Recommendation 3 – NAS Report



Peer-reviewed research on the scientific basis & validity



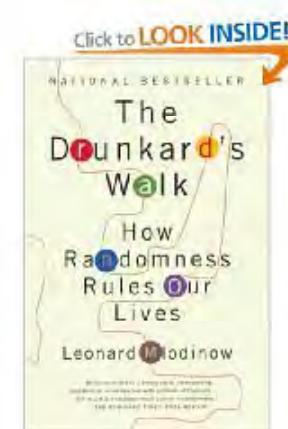
# Wine Tasting



The Wine News, as quoted on wine.com "Dusty, chalky scents followed by mint, plum, tobacco and leather. Tasty cherry with smoky oak accents..."



The Wine Advocate, describes a wine as having "promising aromas of lavender, roasted herbs, blueberries, and black currants."







# Forensics – Information Sharing





# Forensics – Information Sharing

- Logical
- Technical



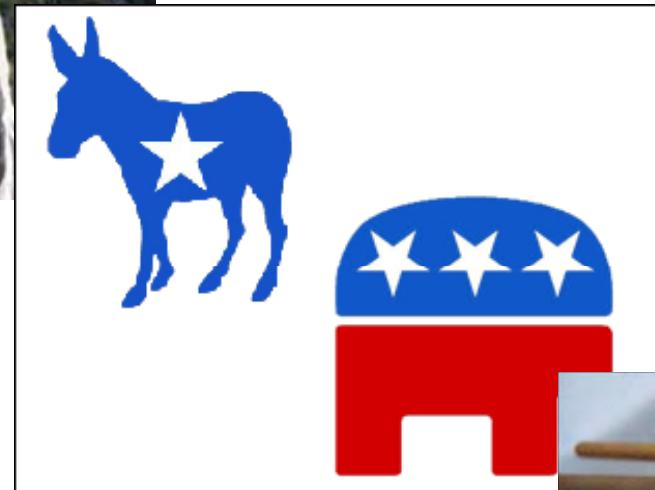
## BANDWIDTH



HOW MUCH IS NEEDED, AND HOW MUCH IS IT WORTH?



PERSONALITY



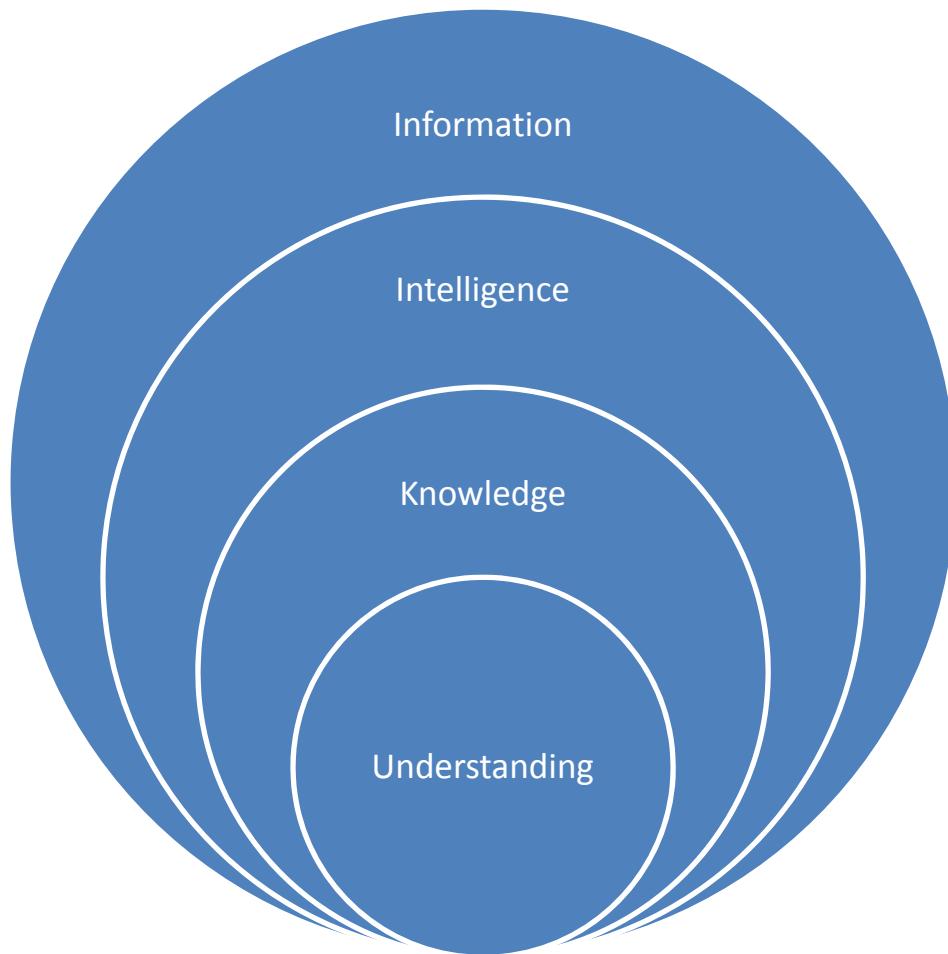
POLITICS



RICE BOWLS



# Forensics – Information Sharing





# Forensic S&T Workshop

MEMORANDUM FOR: SEE DISTRIBUTION  
DIRECTOR OF DEFENSE RESEARCH AND ENGINEERING  
3000 DEFENSE PENTAGON  
WASHINGTON, D.C. 20301-3030  
AUG 3 6 2008  
SUBJECT: Forensic Science and Technology (S&T) Workshop Invitation

Your Analytic Service of this workshop leadership, est desired future to formal acq

The est necessary and Non technical collect, analy, Operations and to identify

At my DoD Com step in define science and to base will be pr

Please do not be asked to provide related S&T in collecting, and workshop is at

Provide the no nicole hawk is this effort is D may reach him

Attachments: As stated

**DoD Forensic Science and Technology Workshop**

Meeting emerging and future needs  
15-17 October 2008

- Engage DOD & interagency leadership
- Establish an S&T baseline for the forensic program
- Map the baseline to desired future capabilities
- Enable a DOD S&T roadmap that defines transition paths to formal acquisition programs

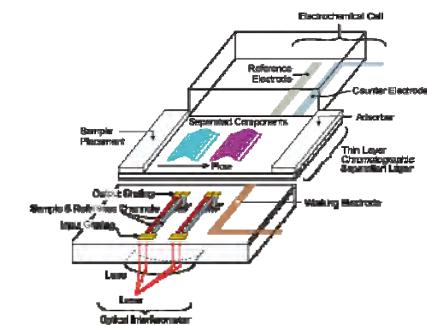
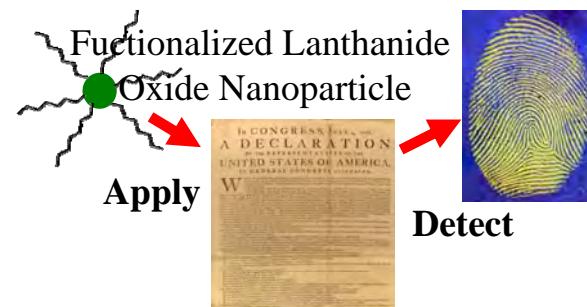
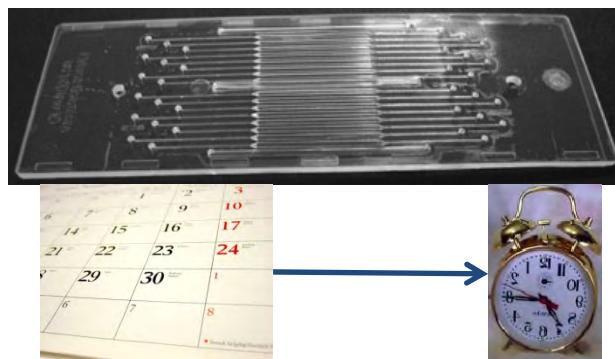
## Outcome

- **25 findings and 34 recommendation**
  - **Identified forensic S&T gaps**
  - **Stand up a Forensic S&T Working Group to address forensics issues and gaps across the community**



# DoD Forensic S&T Current Projects

## ANDE



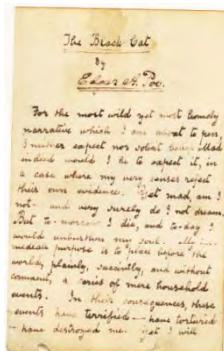
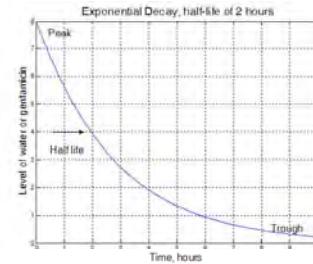
A Single Kit to Screen for Explosives, Drugs, and GSR in the field



UNCLASSIFIED



# DoD Forensic S&T Future Projects



Helen Greey.  
Helen Greey

UNCLASSIFIED

## Man eats underwear to beat breathalyzer

By D'ARCY RICKARD  
of The Advocate

STETTLER — An 18-year-old Stettler man tried to eat his underwear in the hope that his cotton fabric would absorb alcohol before he took a breathalyzer test, provincial court heard this week.

David Zurfluh was subsequently acquitted of a charge of impaired driving because he blew .08, the legal limit.

But the testimony broke up people in Judge David MacNaughton's provincial court here Thursday afternoon.

Mr. Zurfluh was collared by RCMP Const. Bill Robinson after he ran from his vehicle, which had been seen weaving down the highway.

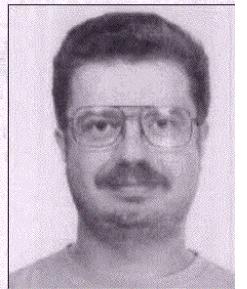
While sitting in the back of the patrol car, Mr. Zurfluh tried to eat his shorts. Const. Robinson told the court:

Mr. Zurfluh said he ripped the crotch out of his shorts, stuffed the fabric in his mouth and then spit it out.

A class of law students from William E. Hay Composite High, in court as observers,

was removed by the teacher when testimony enlivened the proceedings. The Grade 11 and 12 students had difficulty maintaining composure.

"People were leaving the courtroom with tears in their eyes, trying not to laugh," said RCMP Const. Peter McFarlane.





# DoD Forensic S&T Future Questions

- Age of \_\_\_\_\_?
- \_\_\_\_\_ instead of DNA?
- \_\_\_\_\_ to find Gun Shot Residue?
- \_\_\_\_\_ instead of CODIS, IAFIS, NIBN, ...?
- $\pm$  \_\_\_\_\_ and error rate = \_\_\_\_\_ instead of match, consistent with, etc
- \_\_\_\_\_ in min, secs instead of days, weeks, months?



# Summary

- ✓ Centralized vs Decentralized
  - ✓ Faster, Better, Cheaper
  - ✓ NAS Report
  - ✓ Managing Results
- ✓ Gaps
  - ✓ Existing DoD Projects
  - ✓ Future Projects







# National Defense Industrial Association Biometrics Conference Technology and Standards Panel 21 January 2010

DoD Forensic Science & Technology

Jeff Salyards

Program Manager, Science and Technology

U.S. Army Criminal Investigation Laboratory

(404) 469-5569 (office)

[jeff.salyards@us.army.mil](mailto:jeff.salyards@us.army.mil)



# Privacy Issues Fireside Chat

Steve Yonkers, US-VISIT Program

January 20, 2010



Homeland  
Security

**US-VISIT**  
Keeping America's Doors Open and Our Nation Secure

# US-VISIT Overview

- In 2004, US-VISIT became the first, large scale biometric identification program of its kind, enabling the collection of international travelers' biometrics – fingerprints and a digital photograph – at US ports of entry.
- Privacy is an integral part of US-VISIT, and is essential to the program's mission.



Homeland  
Security

**US-VISIT**  
Keeping America's Doors Open and Our Nation Secure

# US-VISIT and Privacy

- US-VISIT's privacy practices are based on The Privacy Act of 1974 which includes Fair Information Practice Principles (FIPPs). The Privacy Act helped US-VISIT set important guidelines for approaching privacy within the organization.
- The US-VISIT privacy program promotes privacy awareness, and builds trust by implementing sound privacy practices. This includes the ten Privacy Principles.



Homeland  
Security

**US-VISIT**  
Keeping America's Doors Open and Our Nation Secure

# US-VISIT Privacy Principles

#1 Responsibility and Accountability

#2 Identifying Purpose

#3 Limiting Collection, Use,  
Disclosure and Retention



Shred it. Secure it. Protect  
it. Privacy. It's our duty.

[www.dhs.gov/privacy](http://www.dhs.gov/privacy)



Homeland  
Security

**US-VISIT**  
Keeping America's Doors Open and Our Nation Secure

# US-VISIT Privacy Principles

#4 Openness and Transparency

#5 Strict Confidentiality

#6 Data Integrity



**Shred it. Secure it. Protect  
it. Privacy. It's our duty.**

[www.dhs.gov/privacy](http://www.dhs.gov/privacy)



Homeland  
Security

**US-VISIT**  
Keeping America's Doors Open and Our Nation Secure

# US-VISIT Privacy Principles

#7 Security

#8 Privacy Awareness and Training

#9 Individual Access



**Shred it. Secure it. Protect  
it. Privacy. It's our duty.**

[www.dhs.gov/privacy](http://www.dhs.gov/privacy)



Homeland  
Security

**US-VISIT**  
Keeping America's Doors Open and Our Nation Secure

# US-VISIT Privacy Principles

## #10 Redress

- Through a robust redress program, US-VISIT gives prompt attention to inquiries and requests for amendment or correction of information that might not be accurate, relevant or current.



**Shred it. Secure it. Protect it.  
Privacy. It's our duty.**

[www.dhs.gov/privacy](http://www.dhs.gov/privacy)



Homeland  
Security

**US-VISIT**  
Keeping America's Doors Open and Our Nation Secure

# US-VISIT Commitment to Privacy

- US-VISIT's Privacy Program is led by a dedicated Privacy Officer with a staff of privacy analysts who are responsible for ensuring compliance with Federal privacy laws and procedures.
- These privacy officials maintain a culture within US-VISIT where privacy is valued, treated as a fundamental right and obligation.



Homeland  
Security

**US-VISIT**  
Keeping America's Doors Open and Our Nation Secure

# US-VISIT Commitment to Privacy

- US-VISIT takes privacy into account during all stages of a project – from conception through planning and development and execution – and every aspect of the program.
- US-VISIT is proud of its privacy culture, but we are acutely aware that the protection of privacy requires constant vigilance and openness.



Homeland  
Security

**US-VISIT**  
Keeping America's Doors Open and Our Nation Secure



# Biometric Screening Programs

Steve Yonkers, US-VISIT Program  
January 20, 2010



Homeland  
Security

**US-VISIT**  
Keeping America's Doors Open and Our Nation Secure

# What is US-VISIT?

In 2004, US-VISIT became the first, large scale biometrics identification program of its kind, enabling the collection of international travelers' biometrics – fingerprints and a digital photograph – at U.S. ports of entry. Today, the U.S. is not alone in recognizing the benefits of biometrics for immigration and border management.



Homeland  
Security

**US-VISIT**  
Keeping America's Doors Open and Our Nation Secure

# Users of US-VISIT's Biometric Identification and Analysis Services



# 2009 Highlights: Completed 10-Fingerprint Collection

- US-VISIT completed its transition from a 2-fingerprint standard to one based on 10 fingerprints.
- Now all ports of entry have the capability to collect up to 10 fingerprints from international travelers.
- This upgrade will increase fingerprint matching accuracy, and provide the ability to check latent fingerprints picked up by local law enforcement as well as DOD in Iraq, Afghanistan, and other parts of the globe against the US-VISIT system.



Homeland  
Security

**US-VISIT**  
Keeping America's Doors Open and Our Nation Secure

# 2009 Highlights: Enhanced Interoperability

- This 10 fingerprint upgrade also complements the work we do with the FBI, making our systems interoperable and allowing for information to be exchanged easily.
- Interoperability also makes initiatives like Secure Communities possible. In 2009, with Immigration and Customs Enforcement (ICE) as the lead agency, US-VISIT was able to provide the necessary support to open 95 sites in 11 States.
- We supported the identification of more than 11,000 criminal aliens charged or convicted of crimes considered to be ICE's top priority, such as rape, homicide and kidnapping.



Homeland  
Security

**US-VISIT**  
Keeping America's Doors Open and Our Nation Secure

# 2009 Highlights: Completed Additional Testing of Biometric Exit Procedures

## Airports and Seaports:

- DHS completed its test of biometric exit procedures at Hartsfield-Jackson Atlanta International Airport and Detroit Metropolitan Wayne County Airport on July 2, 2009.
- DHS will update international travelers about any changes to biometric requirements before they go into effect next year.



## Land Border Ports:

- US-VISIT submitted a report to DHS on opportunities and challenges of deploying biometric exit procedures at land border ports of entry



Homeland  
Security

**US-VISIT**  
Keeping America's Doors Open and Our Nation Secure

# Interoperability

- Improve coordination and interoperability among our government partners that operate biometric identity management programs.
  - Today, US-VISIT's IDENT and the FBI's IAFIS, are interoperable and we continue to make improvements to how these systems work together.
  - We are also working with DOD to make IDENT and DOD's biometric system ABIS interoperable.
    - Currently we incorporate information from ABIS about known or suspected terrorists into the IDENT watchlist.



Homeland  
Security

**US-VISIT**  
Keeping America's Doors Open and Our Nation Secure

# Interoperability

- By 2010, all three systems – IDENT, IAFIS, and ABIS – will be interoperable, making information sharing among these systems more seamless.
- The systems will remain separate and access to the information in each system will continue to be limited to authorized officials with a need for the information.
- But their interoperability will make the biometric matching process more efficient.



Homeland  
Security

**US-VISIT**  
Keeping America's Doors Open and Our Nation Secure

# Multimodal Biometrics

- Last year, US-VISIT completed an evaluation of multimodal biometric technology, including iris recognition, in collaboration with DHS's Science and Technology Directorate and National Institute of Science and Technology (NIST).
- The results of this evaluation are part of a report that's been shared among interested parties in DHS, DOD and NIST, and it serves as a foundation for making identification technologies even more secure and convenient.



Homeland  
Security

**US-VISIT**  
Keeping America's Doors Open and Our Nation Secure

# International Collaboration

- Last year, we continued collaborating with foreign governments seeking to incorporate biometrics into their immigration and border management systems.
- We shared best practices with 19 countries in various stages of implementing biometrics for their immigration systems.



Homeland  
Security

**US-VISIT**  
Keeping America's Doors Open and Our Nation Secure

# International Collaboration

- Also in 2009, we continued to work closely with the UK, Australia and Canada to test limited biometric information sharing in order to expand to more systematic methods for identifying known or suspected criminals and immigration violators.
- We began work with Germany on a fingerprint exchange program.
- We worked with the G8 countries on best practices.
- In partnership with USCIS, we continued our close collaboration with the UK Border Agency.



Homeland  
Security

**US-VISIT**  
Keeping America's Doors Open and Our Nation Secure

# Looking Ahead

- Continue work with the FBI; DOD Interoperability; and continue working with ICE on additional Secure Communities sites.
- Work with increased number of international partners.
- Work with the private sector on new and innovative ways to support our operational stakeholders.
- Prepare for the decision on biometric air exit.



Homeland  
Security

**US-VISIT**  
Keeping America's Doors Open and Our Nation Secure